Universidade de Aveiro Departamento de Matemática
Ano 2009

Ângela Margarida Vergas Ribau

Máquinas Algébricas

Universidade de Aveiro Departamento de Matemática
Ano 2009

Ângela Margarida Vergas Ribau

Máquinas Algébricas

Dissertação apresentada à Universidade de Aveiro para cumprimento dos requisitos necessários à obtenção do grau de Mestre em Matemática e Aplicações, realizada sob a orientação científica do Doutor Manuel António Gonçalves Martins, Professor Auxiliar da Universidade de Aveiro e do Doutor Luís António Arsénio Descalço, Professor Auxiliar da Universidade de Aveiro.

o júri

presidente

Prof. Doutor Domingos Moreira Cardoso
Professor Catedrático da Universidade de Aveiro

Prof. Doutor António José Mesquita Machado da Cunha Malheiro
Professor Auxiliar da Faculdade de Ciências e Tecnologia da Universidade Nova de Lisboa

Prof. Doutor Manuel António Gonçalves Martins
Professor Auxiliar da Universidade de Aveiro

Prof. Doutor Luís António Arsénio Descalço
Professor Auxiliar da Universidade de Aveiro

agradecimentos

Agradeço ao Doutor Manuel António Gonçalves Martins e ao Doutor Luís António Arsénio Descalço, o tempo dispendido na orientação da dissertação e no esclarecimento de dúvidas.

palavras-chave

Álgebra universal heterogénea, primeiro teorema do homomorfismo, autómatos de *Mealy*, autómato quociente, equivalência comportamental.

resumo

Um tópico importante na área de Ciências da Computação é o estudo de problemas que podem ser resolvidos por máquinas como os autómatos ou as máquinas de *Turing*. Este trabalho propõe-se a estudar a teoria de autómatos desenvolvendo para estes uma teoria algébrica, recorrendo a conceitos e resultados da álgebra universal heterogénea.

keywords Universal algebra, first homomorphism theorem, mealy automata, quocient automata, behaviourall equivalence

abstract An important research topic in Computer Science is the study of problems that can be solved by abstract machines like automata or Turing machines. In this work we consider finite state automata and propose an algebraic theory, making use of concepts and results from many-sorted algebra, to study these machines.

Conteúdo

Introdução

Na área de ciências da computação, um tópico importante é o estudo de problemas que podem ser resolvidos por *máquinas*.

Uma *máquina* é um dispositivo mecânico ou orgânico que executa ou ajuda no cumprimento de tarefas. Nesta tese trabalhar–se–á com a definição de máquina, mais propriamente com a definição de máquina num sentido abstracto, uma vez que aqui uma máquina irá ser tratada como uma entidade matemática.

Deste modo, uma *máquina abstracta* é um dispositivo de *input*/*output*, discreto e de estado finito, com um número finito de configurações internas, e que quando lhe é aplicada um conjunto de estímulos, a máquina reenvia um conjunto de respostas. São exemplos de máquinas abstractas, os autómatos, as máquinas de *Turing*, os programas informáticos, etc.

A *teoria de autómatos* é a teoria que nos permite estudar as máquinas abstractas e os problemas que estas podem resolver. Assim, o objectivo desta tese será estudar os autómatos, mais propriamente os autómatos cujo conjunto de estados é finito e desenvolver para estes uma teoria algébrica.

Para desenvolver essa teoria algébrica utilizar–se–á a *álgebra universal heterogénea*, que é uma generalização da álgebra universal, onde em vez de se considerar um único universo para a álgebra é considerada uma família de conjuntos, sendo as funções definidas entre os membros da família.

Deste modo, definir–se–á autómato como uma álgebra heterogénea e verificar–se–á que conceitos como congruência, homomorfismo, isomorfismo, conjunto quociente, etc, se aplicam aos autómatos.

Esta tese encontra-se dividida em dois Capítulos. No Capítulo 1 definir–se–á conceitos e resultados fundamentais da álgebra universal heterogénea, tais como congruência, álgebra quociente, homomorfismo, Primeiro Teorema do Homomorfismo, etc. No Capítulo 2, introduzir–se–á numa primeira fase conceitos iniciais da teoria de autómatos, para depois se definir autómato como uma álgebra heterogénea e se verificar que os conceitos e propriedades do Capítulo 1, lhes são aplicáveis.

Ao longo do texto apresentar–se–á exemplos que complementam a compreensão dos vários conceitos.

Capítulo 1

Elementos de álgebra universal

A álgebra universal tem como principal objectivo o estudo de propriedades que são comuns a diferentes classes de estruturas algébricas. Sendo assim, são estudados vários conceitos, construções e resultados, que para além de generalizarem e de unificarem alguns conceitos que já são conhecidos, permitem um elevado grau de abstracção.

Neste capítulo, descreve–se alguns destes conceitos da álgebra universal, tais como homomorfismo, isomorfismo, congruência, álgebra quociente, etc.

Uma álgebra é um par constituído por um conjunto não vazio, que se designa por *universo* da álgebra e uma família de funções, tendo cada uma dessas funções uma aridade associada.

Para desenvolver uma teoria algébrica para os diferentes autómatos, utilizar–se–á a álgebra universal heterogénea, que é uma generalização da álgebra universal. Neste contexto, em vez de se considerar um único universo considera–se uma família de conjuntos, sendo as funções definidas entre os membros da família. Para tal, será necessário começar por introduzir alguns conceitos da teoria de conjuntos, envolvendo conjuntos heterogéneos.

Os resultados fundamentais deste capítulo poderão ser encontrados em [4] e [9].

1 Conjuntos heterogéneos

Nesta secção introduzir–se–á alguns conceitos da teoria de conjuntos, envolvendo conjuntos heterogéneos.

Seja S um conjunto cujos elementos são designados por *géneros*. Designa–se por S–*conjunto* (ou simplesmente por *conjunto heterogéneo*) uma família de conjuntos indexada por S. No caso em que S é singular, designa–se o S–conjunto por *conjunto homogéneo*.

A notação $A = \langle A_s \rangle_{s \in S}$ representa a família de objectos A_s indexada por $s \in S$, ou seja é uma função com domínio S, que transforma cada $s \in S$ em A_s.

Definição 1.1. Seja $A = \langle A_s \rangle_{s \in S}$ um S–conjunto. Diz-se que A é um *S–conjunto não vazio*, se $A_s \neq \emptyset$ para todo o $s \in S$.

Definição 1.2. Seja $A = \langle A_s \rangle_{s \in S}$ um S–conjunto. Diz-se que A é um *S–conjunto finito*, se A_s é finito para todo o $s \in S$, e existe um conjunto finito $S' \subseteq S$ tal que, $A_s = \emptyset$ para todo o $s \in S \setminus S'$.

Para os conjuntos heterogéneos é possível generalizar alguns conceitos da teoria de conjuntos, tais como: a inclusão, a igualdade, a união, a intersecção e o produto cartesiano. Essa generalização é efectuada componente a componente. Assim, dados S–conjuntos A e B define-se:

$$A \subseteq B \text{ se e só se } A_s \subseteq B_s \text{ para todo o } s \in S$$
$$A = B \text{ se e só se } A_s = B_s \text{ para todo o } s \in S$$
$$A \cup B = \langle A_s \cup B_s \rangle_{s \in S}$$
$$A \cap B = \langle A_s \cap B_s \rangle_{s \in S}$$
$$A \times B = \langle A_s \times B_s \rangle_{s \in S}$$

Definição 1.3. Sejam A e B S–conjuntos da forma $A = \langle A_s \rangle_{s \in S}$ e $B = \langle B_s \rangle_{s \in S}$. Uma *$S$–função* $f : A \longrightarrow B$ consiste numa S–família de funções $f = \langle f_s \rangle_{s \in S}$, com $f_s : A_s \longrightarrow B_s$ para todo o $s \in S$. O conjunto A designa-se por *domínio* de f e o conjunto B por *contradomínio* de f.

Diz–se que uma S–função $f : A \longrightarrow B$ é *sobrejectiva*, *injectiva*, *bijectiva*, se para todo o $s \in S$ $f_s : A_s \longrightarrow B_s$ é, respectivamente, sobrejectiva, injectiva e bijectiva.

Também a composição de funções é definida componente a componente. Ou seja, sendo $f : A \longrightarrow B$ e $g : B \longrightarrow C$ duas S–funções, a *função composta* $g \circ f : A \longrightarrow C$ é a S–função definida por:

$$(g \circ f)_s(a) = (g_s \circ f_s)(a) = g_s(f_s(a)) \tag{1.1}$$

para todo o $s \in S$ e $a \in A_s$.

Definição 1.4. Seja $A = \langle A_s \rangle_{s \in S}$ um S–conjunto. A relação $R \subseteq A \times A$ é uma *S–relação binária* em A, se consiste numa S–família $R = \langle R_s \rangle_{s \in S}$ tal que, $R_s \subseteq A_s \times A_s$ para todo o $s \in S$.

Seja A um conjunto homogéneo não vazio. Uma relação binária $\theta \subseteq A \times A$ é uma *relação de equivalência* em A, se θ é reflexiva, simétrica e transitiva. O conjunto de todas as relações de equivalência em A é denotado por $Eq(A)$.

A relação de equivalência $\{(a, a) : a \in A\}$ é designada por *diagonal* de A e denota–se por $\triangle_A$. Esta relação é a relação de igualdade definida em qualquer conjunto A.

Dada uma relação de equivalência θ sobre A e $x \in A$, define–se a *classe de equivalência relativa a* x como o conjunto de todos os elementos de A equivalentes a x, ou seja

$$x/\theta = \{y \in A \ : \ y \ \theta \ x\}.$$

Define–se também *conjunto quociente* de A por θ, como o conjunto de todas as classes de equivalência determinadas em A por θ. O conjunto quociente de A por θ é dado por:

$$A/\theta = \{x/\theta \ : \ x \in A\}.$$

Uma forma alternativa de abordar relações de equivalência é através de partições.

Uma *partição* π de A é um conjunto de subconjuntos não vazios de A, tais que todo o elemento de A pertence exactamente a um desses subconjuntos. Esses subconjuntos são designados por *blocos* da partição. Formalmente, uma partição π é um conjunto tal que:

– $A = \bigcup\{X : X \in \pi\}$;

– Se $X, Y \in \pi$ então ou $X = Y$ ou $X \cap Y = \emptyset$.

O conjunto de todas as partições de um conjunto A é denotado por $\Pi(A)$.

Considere–se $\pi \in \Pi(A)$. Define–se a relação de equivalência $\theta(\pi)$ por:

$$\theta(\pi) = \{(a, b) \in A \times A \ : \ \{a, b\} \subseteq B \text{ para algum } B \in \pi\}.$$

Observa-se que a aplicação $\pi \longmapsto \theta(\pi)$ é uma bijecção entre $\Pi(A)$ e $Eq(A)$. Formalmente, isto significa que a partição π induz uma relação de equivalência que é $\theta(\pi)$, e por sua vez a relação de equivalência θ induz uma partição π_θ, tal que $\pi_\theta = A/\theta$. Portanto, a noção de partição e de relação de equivalência estão intimamente relacionadas.

Depois de relembrados estes conceitos, define–se de seguida *relação de equivalência* e *conjunto quociente*, para conjuntos heterogéneos.

Definição 1.5. Seja A um S–conjunto e $\equiv = \langle \equiv_s \rangle_{s \in S}$ uma S–relação binária em A. A relação $\equiv$ é uma *S–relação de equivalência* ou simplesmente *relação de equivalência* em A, se para todo o $s \in S$ $\equiv_s$ é uma relação de equivalência em A_s.

Definição 1.6. Seja A um S–conjunto e $\equiv = \langle \equiv_s \rangle_{s \in S}$ uma S–relação de equivalência em A. O *conjunto quociente* de A módulo $\equiv$ é o S-conjunto

$$A/\equiv = \langle A_s/\equiv_s \rangle_{s \in S}.$$

2 Assinaturas e álgebras

Nesta secção apresentar–se–á alguns conceitos de álgebra universal heterogénea, os quais permitirão efectuar a passagem para o que se pretende efectuar no Capítulo 2.

Começa–se por definir uma *assinatura*.

Definição 1.7. Uma *assinatura* Σ é um par $\langle S, \Omega \rangle$ onde:

- S é um conjunto, designado por *conjunto dos géneros*;
- Ω é um $(S^* \times S)$–conjunto, que é o *conjunto de nomes* ou *símbolos*, de *operação* ou *função*, onde S^* representa o conjunto de todas as sequências finitas de elementos de S, incluindo a sequência vazia.

Os símbolos em $\Omega_{s_1 s_2 \ldots s_n, s}$, com $n \geq 1$, são os *símbolos funcionais* com os *argumentos* de géneros $s_1, \ldots, s_n$, e *resultado* de género s. Os elementos de $\Omega_{\varepsilon, s}$ com $s \in S$, são as *constantes* de género s, onde ε representa a sequência vazia de S^*. Um símbolo de operação $f \in \Omega_{s_1 s_2 \ldots s_n, s}$ pode ser representado por $f : s_1, \ldots, s_n \longrightarrow s \in \Sigma$ com $s_1, \ldots, s_n, s \in S$. Por sua vez, $s_1, \ldots, s_n \longrightarrow s$ designa-se por *tipo* de f.

Exemplo 1.8. Considere–se uma célula de memória num computador, na qual se pode ler e armazenar valores. Este sistema pode ser especificado pela assinatura $\Sigma_{cell} = \langle S, \Omega \rangle$ onde $S = \{\texttt{elt}, \texttt{cell}\}$, sendo o género `elt` o que representa os valores a armazenar na célula e o género `cell` o que representa as células propriamente ditas, e onde $\Omega_{\texttt{elt cell},\texttt{cell}} = \{\texttt{put}\}$, $\Omega_{\texttt{cell},\texttt{elt}} = \{\texttt{get}\}$ e $\Omega_{w,a} = \emptyset$ para os outros casos, com `put` a representar a função que armazena um valor `elt` numa célula `cell` e com `get` a representar a função que lê o valor armazenado em `cell`. Assim, estas funções são especificadas por, $\texttt{put} : \texttt{elt}, \texttt{cell} \longrightarrow \texttt{cell}$ e $\texttt{get} : \texttt{cell} \longrightarrow \texttt{elt}$, como ilustra a Figura 1.1. ♢

Introduz-se de seguida a noção de Σ–*álgebra*. As Σ–álgebras são entidades semânticas que dão sentido ou interpretação aos géneros e símbolos de função de uma assinatura.

Definição 1.9. Seja $\Sigma = \langle S, \Omega \rangle$ uma assinatura. Uma Σ–*álgebra* $\mathcal{A}$ consiste num S–conjunto $A = \langle A_s \rangle_{s \in S}$ não vazio e, para cada símbolo $f : s_1, \ldots, s_n \longrightarrow s \in \Sigma$ tem-se uma função,

$$f^{\mathcal{A}} : A_{s_1} \times \ldots \times A_{s_n} \longrightarrow A_s.$$

Denota–se $\mathcal{A}$ por

$$\mathcal{A} = (A, \langle f^{\mathcal{A}} \rangle_{f \in \Omega}).$$

O S–conjunto A designa-se por *universo* ou *domínio* de $\mathcal{A}$.

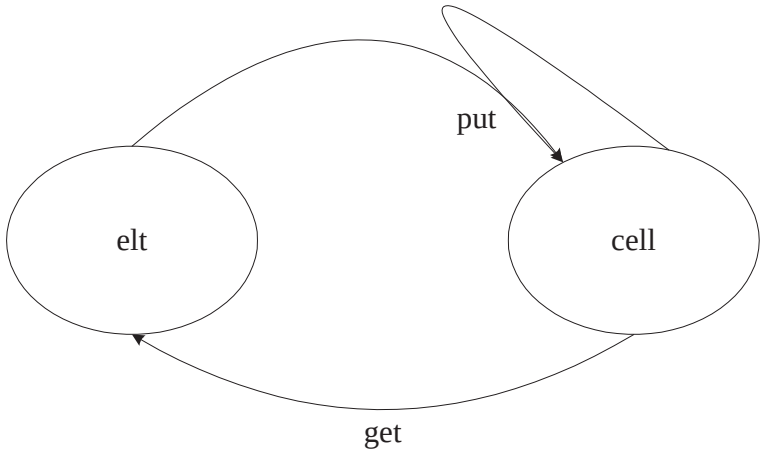


Figura 1.1: Diagrama da assinatura Σ_{cell}.

Quando Ω é finito isto é, quando $\Omega = \{f_1, \ldots, f_n\}$, a Σ–álgebra denota-se por

$$\mathcal{A} = (A, f_1^{\mathcal{A}}, \ldots, f_n^{\mathcal{A}}).$$

Seja $f : s_1, \ldots, s_n \longrightarrow s \in \Sigma$. Quando $n = 0$, f é uma constante denotada por $f : \longrightarrow s \in \Sigma$, e neste caso $A_{s_1} \times \ldots \times A_{s_n}$ é um conjunto singular, cujo único elemento é o tuplo vazio ( ). Logo, $f^{\mathcal{A}}$ pode ser visto como um elemento distinguido de A_s, que denota o valor da função $f^{\mathcal{A}}(( )) \in A_s$.

Na definição de Σ–álgebra, o universo é um S–conjunto não vazio, ou seja tem todas as componentes não vazias. Para além disso, as funções são totais.

Em muitos casos identifica–se os nomes das operações com as suas interpretações.

No caso em que se tem apenas um género, designa–se a Σ–álgebra por *álgebra homogénea*. Alguns resultados a apresentar ao longo do texto, só têm interesse para este tipo de álgebra. Portanto, sempre que for claro no contexto assumir–se–á implicitamente este facto.

Exemplo 1.10. O par $\mathcal{A} = (A, \langle f^{\mathcal{A}} \rangle_{f \in \Omega})$ com o universo definido por $A_{\texttt{elt}} = \mathbb{N}$, $A_{\texttt{cell}} = \{[n] \ : \ n \in \mathbb{N}\}$ e as funções por $\texttt{get}^{\mathcal{A}}([n]) = n$ e $\texttt{put}^{\mathcal{A}}(m, [n]) = [m]$, é uma Σ_{cell}–álgebra. ♢

3 Congruências e álgebras quocientes

Uma construção importante em álgebra universal, é a construção do quociente associada a uma relação de equivalência num conjunto ou numa Σ–álgebra. Para efectuar essa

construção, começa–se por definir *relação de congruência*.

Definição 1.11. Seja $\Sigma = \langle S, \Omega \rangle$ uma assinatura e $\mathcal{A}$ uma Σ–álgebra. Uma *congruência* em $\mathcal{A}$ é uma S–relação de equivalência em A não vazia, $\langle \equiv_s \rangle_{s \in S}$ tal que, para qualquer $f : s_1, \ldots, s_n \longrightarrow s \in \Sigma$, e quaisquer $a_i, b_i \in A_{s_i}$ com $i \in \{1, \ldots, n\}$ se, $a_i \equiv_{s_i} b_i$ para todo o $i \leq n$, então

$$f^{\mathcal{A}}(a_1, \ldots, a_n) \equiv_s f^{\mathcal{A}}(b_1, \ldots, b_n).$$

O conjunto de todas as congruências em $\mathcal{A}$ é denotado por $Con(\mathcal{A})$.

Exemplo 1.12. Normalmente não se trabalha directamente com as congruências. Por exemplo, na teoria dos grupos são os subgrupos normais que desempenham o papel das congruências. Ou seja:

Seja G um grupo[1]. Então pode–se estabelecer uma relação entre as congruências em G e os subgrupos normais [2] de G:

1. Se $\theta \in Con(G)$ então $1/\theta$ é um subgrupo normal de G, e para quaisquer $a, b \in G$, $\langle a, b \rangle \in \theta \Leftrightarrow a \cdot b^{-1} \in 1/\theta$, onde $1/\theta$ denota a classe de equivalência da identidade do grupo.

2. Se N é um subgrupo normal de G, então a relação binária definida em G por $\langle a, b \rangle \in \theta \Leftrightarrow a \cdot b^{-1} \in N$ é uma congruência em G, com $1/\theta = N$. ♢

A propriedade apresentada na Definição 1.11 é denominada por *propriedade de compatibilidade* e vai permitir munir o conjunto quociente $A/\equiv$ com estrutura de Σ–álgebra induzida pela Σ–álgebra $\mathcal{A}$.

Sejam $f : s_1, \ldots, s_n \longrightarrow s \in \Sigma$ e $a_1 \in A_{s_1}, \ldots, a_n \in A_{s_n}$. Aplicando f a $\langle a_1/\equiv_{s_1}, \ldots, a_n/\equiv_{s_n} \rangle$, a escolha apropriada para a classe do valor obtido é:

$$f^{\mathcal{A}}(a_1, \ldots, a_n)/\equiv_s .$$

Define–se assim Σ–*álgebra quociente* como se segue:

Definição 1.13. Seja $\mathcal{A}$ uma Σ–álgebra e $\equiv$ uma congruência em $\mathcal{A}$. A *álgebra quociente* de $\mathcal{A}$ por $\equiv$ é a Σ–álgebra $\mathcal{A}/\equiv$ definida por:

– $\big(A/\equiv\big)_s = A_s/\equiv_s$ para todo o $s \in S$;

– para cada $f : s_1, \ldots, s_n \longrightarrow s \in \Sigma$ e quaisquer $a_1 \in A_{s_1}, \ldots, a_n \in A_{s_n}$,

$$f^{\mathcal{A}/\equiv}(a_1/\equiv_{s_1}, \ldots, a_n/\equiv_{s_n}) = f^{\mathcal{A}}(a_1, \ldots, a_n)/\equiv_s .$$

[1] Recorde–se que um grupo é um par ordenado $(G, *)$ onde: $G \neq \emptyset$, $*$ é uma operação binária, que é associativa, admite elemento neutro e cada elemento de G tem elemento inverso

[2] E diz–se que N é um subgrupo normal de G se $aN = Na$, para qualquer $a \in G$.

4 Homomorfismos e isomorfismos

Neste momento, formular–se–á conceitos que permitem relacionar duas Σ–álgebras $\mathcal{A}$ e $\mathcal{B}$. Em particular, definir–se–á o que quer dizer $\mathcal{A}$ e $\mathcal{B}$ serem estruturalmente idênticas ou isomorfas, como Σ–álgebras.

Começa–se esta secção definindo os conceitos de *homomorfismo*, *epimorfismo*, *isomorfismo*, *endomorfismo* e *automorfismo*.

Definição 1.14. Sejam $\Sigma = \langle S, \Omega \rangle$ uma assinatura e $\mathcal{A}$ e $\mathcal{B}$ duas Σ–álgebras. Um Σ–*homomorfismo*, ou simplesmente *homomorfismo*, $h : \mathcal{A} \longrightarrow \mathcal{B}$ é uma S–função $\langle h_s : A_s \longrightarrow B_s \rangle_{s \in S}$ tal que, para qualquer símbolo funcional $f : s_1, \ldots, s_n \longrightarrow s \in \Sigma$ e para quaisquer $a_1 \in A_{s_1}, \ldots, a_n \in A_{s_n}$ tem–se:

$$h_s(f^{\mathcal{A}}(a_1, \ldots, a_n)) = f^{\mathcal{B}}(h_{s_1}(a_1), \ldots, h_{s_n}(a_n)).$$

Note–se que na definição anterior, para uma operação constante $f : \longrightarrow s$, tem–se que $h_s(f^{\mathcal{A}}) = f^{\mathcal{B}}$.

Diz–se que o Σ–homomorfismo h é um *epimorfismo*, se h é sobrejectivo e neste caso, a Σ–álgebra $\mathcal{B}$ denomina–se por *imagem homomorfa de* $\mathcal{A}$. Por sua vez, o Σ–homomorfismo h é um *isomorfismo* se h é sobrejectivo e injectivo.

No caso em que $\mathcal{A} = \mathcal{B}$, o Σ–homomorfismo h designa–se por *endomorfismo*. E quando $\mathcal{A} = \mathcal{B}$ e h é um isomorfismo, designa–se h por *automorfismo*.

Se existir um isomorfismo $h : \mathcal{A} \longrightarrow \mathcal{B}$, então diz–se que $\mathcal{A}$ é isomorfo a $\mathcal{B}$, e escreve–se $\mathcal{A} \cong \mathcal{B}$.

Sendo $h : \mathcal{A} \longrightarrow \mathcal{A}$ um isomorfismo, diz–se que h é o *isomorfismo identidade* se $h_s(a) = a$ para todo o $s \in S$ e para todo o $a \in \mathcal{A}$.

Seja $h : \mathcal{A} \longrightarrow \mathcal{B}$ um isomorfismo. Designa–se a S–família $\langle h_s^{-1} : B_s \longrightarrow A_s \rangle_{s \in S}$ por *isomorfismo inverso* (observe–se que para cada $s \in S$, h_s^{-1} existe, pois h_s é bijectiva e satisfaz a propriedade do homomorfismo).

Exemplo 1.15. Um homomorfismo comum é o homomorfismo do grupo aditivo dos inteiros $Z = \langle \mathbb{Z}, +, -, 0 \rangle$ no grupo dos inteiros módulo n, $Z_n = \langle \mathbb{Z}_n, +_n, -_n, 0_n \rangle$ definido por $h(z) = z_n$, onde z_n é a classe do número inteiro z módulo n. $\diamondsuit$

Teorema 1.16. *Sejam $\mathcal{A}$, $\mathcal{B}$ e $\mathcal{C}$ Σ–álgebras e sejam $g : \mathcal{A} \longrightarrow \mathcal{B}$ e $h : \mathcal{B} \longrightarrow \mathcal{C}$ Σ–homomorfismos. Então $h \circ g : \mathcal{A} \longrightarrow \mathcal{C}$ é um Σ–homomorfismo.*

Demonstração. Seja $f : s_1, \ldots, s_n \longrightarrow s \in \Sigma$ um símbolo funcional e sejam $a_1 \in A_{s_1}$,

$\ldots, a_n \in A_{s_n}$. Então tem–se:

$$\begin{aligned}(h \circ g)_s(f^{\mathcal{A}}(a_1, \ldots, a_n)) &= h_s(g_s(f^{\mathcal{A}}(a_1, \ldots, a_n))), \text{ por (1.1)} \\ &= h_s(f^{\mathcal{B}}(g_{s_1}(a_1), \ldots, g_{s_n}(a_n))), \text{ pois } g \text{ é um homomorfismo} \\ &= f^{\mathcal{C}}(h_{s_1}(g_{s_1}(a_1)), \ldots, h_{s_n}(g_{s_n}(a_n))), \text{ pois } h \text{ é um homomorfismo} \\ &= f^{\mathcal{C}}((h \circ g)_{s_1}(a_1), \ldots, (h \circ g)_{s_n}(a_n)), \text{ por (1.1)}\end{aligned}$$

Logo, $h \circ g$ é um Σ–homomorfismo. □

Definição 1.17. Sejam $\mathcal{A}$ e $\mathcal{B}$ Σ–álgebras e $\alpha : \mathcal{A} \longrightarrow \mathcal{B}$ um Σ–homomorfismo. O *núcleo de* α, $\ker(\alpha)$, é uma S–relação binária em A, definida para cada $s \in S$ e para todo $a, b \in A_s$ por:

$$a \ (\ker(\alpha))_s \ b \Leftrightarrow \alpha_s(a) = \alpha_s(b).$$

Teorema 1.18. *Seja $\alpha : \mathcal{A} \longrightarrow \mathcal{B}$ um Σ–homomorfismo. Então, o núcleo de α é uma congruência em $\mathcal{A}$.*

Demonstração. Não é difícil verificar que o núcleo de α é uma S–relação de equivalência em A.

Suponha–se que para $i \in \{1, \ldots, n\}$ tem–se, $a_i \ (\ker(\alpha))_{s_i} \ b_i$. Então, pela definição de núcleo para $i \in \{1, \ldots, n\}$ vem que, $\alpha_{s_i}(a_i) = \alpha_{s_i}(b_i)$. Como α é um Σ–homomorfismo então:

$$\begin{aligned}\alpha_s(f^{\mathcal{A}}(a_1, \ldots, a_n)) &= f^{\mathcal{B}}(\alpha_{s_1}(a_1), \ldots, \alpha_{s_n}(a_n)) \\ &= f^{\mathcal{B}}(\alpha_{s_1}(b_1), \ldots, \alpha_{s_n}(b_n)), \text{ pois } \alpha_{s_i}(a_i) = \alpha_{s_i}(b_i) \\ &= \alpha_s(f^{\mathcal{A}}(b_1, \ldots, b_n)), \text{ pois } \alpha \text{ é um } \Sigma\text{–homomorfismo.}\end{aligned}$$

Deste modo,

$$\alpha_s(f^{\mathcal{A}}(a_1, \ldots, a_n)) = \alpha_s(f^{\mathcal{A}}(b_1 \ldots, b_n)).$$

Então por definição, $f^{\mathcal{A}}(a_1, \ldots, a_n) \ (\ker(\alpha))_s \ f^{\mathcal{A}}(b_1, \ldots, b_n)$. E fica assim provado que o núcleo de α é uma congruência em $\mathcal{A}$. □

Define–se agora *aplicação canónica*.

Definição 1.19. Seja $\mathcal{A}$ uma Σ–álgebra e θ uma congruência em $\mathcal{A}$. A *aplicação canónica* ou *natural* é a S–aplicação $\nu_\theta : A \longrightarrow A/\theta$ definida por:

$$(\nu_\theta)_s(a) = a/\theta_s$$

para todo o $s \in S$ e $a \in A_s$.

Proposição 1.20. *Seja $\mathcal{A}$ uma Σ–álgebra e θ uma congruência em $\mathcal{A}$. A* aplicação canónica *ou* natural *$\nu_\theta : A \longrightarrow A/\theta$ é um Σ–homomorfismo sobrejectivo.*

Demonstração. Seja θ uma congruência em $\mathcal{A}$ e $\nu_\theta : A \longrightarrow A/\theta$ a aplicação natural. Seja $f : s_1, \ldots, s_n \longrightarrow s \in \Sigma$ um símbolo funcional e sejam $a_1 \in A_{s_1}, \ldots, a_n \in A_{s_n}$. Então,

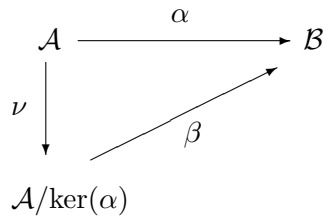
$$\begin{aligned}(\nu_\theta)_s(f^{\mathcal{A}}(a_1,\ldots,a_n)) &= (f^{\mathcal{A}}(a_1,\ldots,a_n))/\theta_s, \text{ por definição de } \nu_\theta \\ &= f^{\mathcal{A}/\theta_s}(a_1/\theta_{s_1},\ldots,a_n/\theta_{s_n}), \text{ por definição de álgebra quociente} \\ &= f^{\mathcal{A}/\theta_s}(\nu_{\theta_{s_1}}(a_1),\ldots,\nu_{\theta_{s_n}}(a_n)), \text{ por definição de } \nu_\theta.\end{aligned}$$

Logo, ν_θ é um Σ–homomorfismo e é claramente sobrejectivo. □

Este Σ–homomorfismo designa-se por Σ–*homomorfismo canónico* ou *natural*.

Enuncia–se agora o *Primeiro Teorema do Homomorfismo*.

Teorema 1.21. *Sejam $\mathcal{A}$ e $\mathcal{B}$ duas Σ–álgebras e $\alpha : \mathcal{A} \longrightarrow \mathcal{B}$ um Σ–homomorfismo sobrejectivo. Então, existe um isomorfismo $\beta : \mathcal{A}/\ker(\alpha) \longrightarrow \mathcal{B}$ tal que, $\alpha = \beta \circ \nu$ e onde $\nu : \mathcal{A} \longrightarrow \mathcal{A}/\ker(\alpha)$ é o Σ–homomorfismo natural.*



Demonstração. A prova deste teorema irá ser efectuada para o caso homogéneo, para assim simplificar a notação. No caso geral o argumento é o mesmo, apenas tem que se efectuar para cada uma das componentes.

Seja $\beta : \mathcal{A}/\ker(\alpha) \longrightarrow \mathcal{B}$ a aplicação

$$\beta(a/\ker(\alpha)) = \alpha(a). \tag{1.2}$$

Começa–se por provar que a aplicação β está bem definida. Para isso, considere–se $a, b \in \mathcal{A}$ tais que, $a/\ker(\alpha) = b/\ker(\alpha)$. Pela definição de núcleo vem que: $\alpha(a) = \alpha(b)$. Pela forma como β foi definida resulta então que, $\beta(a/\ker(\alpha)) = \beta(b/\ker(\alpha))$ e deste modo, verifica–se que β se encontra bem definida. Assim, considerando $a \in \mathcal{A}$

$$\begin{aligned}(\beta \circ \nu)(a) &= \beta(\nu(a)), \text{ por (1.1)} \\ &= \beta(a/\ker(\alpha)), \text{ pela definição de } \nu \\ &= \alpha(a) \text{ pela definição de } \beta.\end{aligned}$$

Portanto, $\alpha = \beta \circ \nu$ para todo o $a \in \mathcal{A}$. Prova–se agora que β é bijectiva. Sabe–se que α é uma aplicação sobrejectiva. Portanto, pela forma como β está definida, pode–se concluir que β é também uma aplicação sobrejectiva. Para provar que β é

uma aplicação injectiva, considere–se $a/\ker(\alpha), b/\ker(\alpha) \in \mathcal{A}/\ker(\alpha)$ quaisquer e tais que, $\beta(a/\ker(\alpha)) = \beta(b/\ker(\alpha))$. Assim, pela definição de β, $\alpha(a) = \alpha(b)$. Mas, pela definição de núcleo vem que: $a\ (\ker(\alpha))\ b$. E portanto, $a/\ker(\alpha) = b/\ker(\alpha)$. E deste modo, conclui–se que β é uma aplicação injectiva. Consequentemente fica provado que β é uma aplicação bijectiva. Falta agora provar que β é um Σ–homomorfismo. Para isso, considere–se f um símbolo funcional n–ário em Σ e $a_1, \ldots, a_n \in A$. Assim:

$$\begin{aligned}
&\beta(f^{\mathcal{A}/\ker(\alpha)}(a_1/\ker(\alpha), \ldots, a_n/\ker(\alpha))) \\
&\qquad = \beta(f^{\mathcal{A}}(a_1, \ldots, a_n)/\ker(\alpha)),\ \text{por definição de } \mathcal{A}/\ker(\alpha) \\
&\qquad = \alpha(f^{\mathcal{A}}(a_1, \ldots, a_n)),\ \text{por (1.2)} \\
&\qquad = f^{\mathcal{B}}(\alpha(a_1), \ldots, \alpha(a_n)),\ \text{pois } \alpha \text{ é um homomorfismo} \\
&\qquad = f^{\mathcal{B}}(\beta(a_1/\ker(\alpha)), \ldots, \beta(a_n/\ker(\alpha))),\ \text{por (1.2)}.
\end{aligned}$$

Deste modo, β é isomorfismo. □

Capítulo 2

Autómatos finitos

Uma parte importante da área de ciências da computação é o estudo de problemas que podem ser resolvidos por *máquinas*.

Uma *máquina* é todo o dispositivo mecânico ou orgânico, que executa ou ajuda no desempenho de tarefas. Para este trabalho, a palavra máquina terá um sentido abstracto, uma vez que irá ser tratada como uma entidade matemática.

Assim, uma *máquina abstracta* é um mecanismo de *input/output*, discreto e de estado finito, que tem um número finito de possibilidades de configurações internas e que quando lhe é aplicada uma colecção de estímulos, tais como premir um botão ou inserir uma moeda, a máquina devolve uma colecção de respostas, como por exemplo aparecer um conjunto de caracteres num écran ou sair um copo de café. São exemplos de máquinas abstractas, os autómatos, as máquinas de *Turing*, os processadores, entre outros.

Para estudar algumas máquinas abstractas e os problemas que estas podem resolver, foi desenvolvida uma teoria: a *teoria dos autómatos*.

Neste capítulo pretende–se efectuar um estudo sobre autómatos. Esse estudo será efectuado de um ponto de vista algébrico, uma vez que considerar–se–á os autómatos como sendo álgebras heterogéneas e desse modo, verificar–se–á que os conceitos e as propriedades descritas no Capítulo 1 lhes são aplicáveis. Em particular, analisar–se–á os autómatos cujo conjunto de estados é finito, uma vez que são estes que modelam a generalidade das máquinas reais. Esses autómatos designam–se por *autómatos finitos*.

Para iniciar este capítulo, começar–se–á por introduzir algumas definições e conceitos, que serão importantes para perceber como é que os autómatos finitos se comportam.

Os resultados fundamentais deste capítulo poderão ser encontrados em [7] e [11].

1 Autómatos finitos: tipos e exemplos

Começa–se esta secção, introduzindo conceitos gerais da teoria de autómatos.

Seja A um conjunto não vazio. Define–se uma *palavra* sobre A, como uma função

$$w : \{1, \ldots, n\} \longrightarrow A$$

para algum número inteiro positivo, n.

A n chama–se *comprimento* de w e denota–se por $|w|$. Se $n = 0$, então convenciona–se que $\{1, \ldots, n\} = \emptyset$ e assim, $w : \emptyset \longrightarrow A$ é a função vazia, que é denotada por ε e designada por *palavra vazia*. Deste modo, $|\varepsilon| = 0$.

Designa–se o conjunto A por *alfabeto* e denota–se o conjunto das palavras sobre A por A^*.

Pode–se pensar em w como a palavra que denota a sequência $w(1) \ldots w(n)$ e usar esta notação para representar as palavras. Assim, escreve–se $a_1 \ldots a_n$ para referir a função w, cujo domínio é $\{1, \ldots, n\}$ e é tal que, $w(i) = a_i$ para $i \in \{1, \ldots, n\}$. Mais à frente, apresentar–se–á algumas definições, para as quais é útil observar que, qualquer palavra em A^* ou é a palavra vazia, ε ou é da forma aw, para alguns $a \in A$ e $w \in A^*$.

Em A^*, pode–se definir a operação *concatenação*. Considere–se $w_1, w_2 \in A^*$. A concatenação de w_1 com w_2, que se denota por $w_1 \cdot w_2$ é a palavra w tal que, $|w| = |w_1| + |w_2|$ e satisfaz:

$$w(i) = \begin{cases} w_1(i) & \text{se } i \leq |w_1| \\ w_2(i - |w_1|) & \text{se } i > |w_1| \end{cases}$$

De um modo mais informal, se $w_1 = a_1 \ldots a_n$ e $w_2 = b_1 \ldots b_m$ então

$$w_1 \cdot w_2 = a_1 \ldots a_n \cdot b_1 \ldots b_m = a_1 \ldots a_n b_1 \ldots b_m,$$

com $n, m \in \mathbb{N}$. Por vezes escreve–se $w_1 w_2$, em vez de $w_1 \cdot w_2$ para $w_1, w_2 \in A^*$.

Como ε é a palavra vazia, verifica–se que:

$$w_1 \cdot \varepsilon = a_1 \ldots a_n \cdot \varepsilon = a_1 \ldots a_n, \text{ com } n \in \mathbb{N}$$

A operação concatenação é uma operação associativa. Portanto, para quaisquer w_1, w_2, $w_3 \in A^*$ tem–se:

$$(w_1 \cdot w_2) \cdot w_3 = w_1 \cdot (w_2 \cdot w_3).$$

Um subconjunto de A^* designa–se por *linguagem*. Dadas duas linguagens $L, K \subseteq A^*$ pode–se definir a *concatenação de duas linguagens* L e K por:

$$L \cdot K = \{w_1 \cdot w_2 : w_1 \in L, w_2 \in K\}.$$

Normalmente, escreve–se LK, em vez de, $L \cdot K$.

As potências L^n são definidas recursivamente por:

$$\begin{aligned} L^0 &= \{\varepsilon\} \\ L^{n+1} &= L \cdot L^n, \text{ com } n \in \mathbb{N}_0 \end{aligned}$$

Para uma linguagem $L \subseteq A^*$ define–se a operação *fecho de Kleene* por:

$$L^* = \bigcup_{n=0}^{\infty} L^n \Big(= \{w_1 \cdot w_2 \cdot \ldots \cdot w_n : w_1, w_2, \ldots, w_n \in L, n \in \mathbb{N}_0\}\Big).$$

Dadas duas linguagens $L, K \subseteq A^*$ define–se também a *união de linguagens*, como uma operação binária, que consiste na união dos conjuntos, que definem cada uma das linguagens.

Conhecendo estes conceitos iniciais sobre linguagens, define–se agora os vários tipos de autómatos.

Na literatura, quando se definem os vários tipos de autómatos, normalmente começa–se pela definição de autómato finito determinístico, depois define–se autómato finito não–determinístico e de seguida definem–se os autómatos finitos com *output*.

O nosso objectivo é definir os autómatos como álgebras heterogéneas e desenvolver uma teoria geral, baseada nos conceitos e propriedades referidos no Capítulo 1, e que suporte alguns dos resultados principais relativos a estes tipos de autómatos. Portanto, começar–se–á por definir autómato finito com *output* e a partir deste definir–se–á autómato finito determinístico e não–determinístico, conseguindo deste modo uma maior generalidade no estudo das diversas máquinas abstractas.

Um *autómato* é uma máquina, que é determinada pelo *conjunto de estados* Z, o *alfabeto de input* I, o *alfabeto de output* O, a função que descreve como os *inputs* provocam uma mudança de estado no autómato, que se designa por *função de transição de estados* e se denota por δ, a função que diz qual o *output* que está associado a cada transição de estados para qualquer *input*, que se designa por *função de outputs* e se denota por β e o estado inicial $z_0 \in Z$. Formalmente, um autómato $\mathcal{M}$ é um sêxtuplo ordenado, que se representa do seguinte modo:

$$\mathcal{M} = (Z, I, O, \delta, \beta, z_0).$$

De seguida, descreve–se que tipo de alterações as funções δ e β provocam no autómato.

Considere–se $z \in Z$ como sendo o estado em que o autómato se encontra e $i \in I$ como sendo o *input* que é fornecido ao autómato. A função de transição δ recebe o par (z, i),

e determina $z^{'} \in Z$ como sendo o novo estado do autómato. Assim, o autómato passa a estar no estado $\delta(z, i) = z^{'} \in Z$. A função δ é da forma:

$$\delta : Z \times I \longrightarrow Z.$$

Quanto à função β, esta determina os *outputs* gerados pelo autómato quando este se encontra num estado $z \in Z$ e recebe um *input* $i \in I$. Assim, a função β também recebe o par (z, i) e determina o *output* $\beta(z, i) = o \in O$. Portanto, a função β é da forma:

$$\beta : Z \times I \longrightarrow O.$$

Um autómato pode ser representado de duas formas: através de um *diagrama de transições* ou através de uma *tabela de transições*.

Em seguida, apresenta–se um exemplo de um autómato, onde se efectua as duas representações, mas nos próximos exemplos apresentar–se–á apenas o diagrama de transições.

Exemplo 2.1. Seja $\mathcal{M} = (Z, I, O, \delta, \beta, z_0)$ o autómato, tal que: $Z = \{q_0, q_1, q_2\}$, $I = \{a, b, c\}$, $O = \{0, 1\}$, $z_0 = q_0$, a função δ definida por:

$$\delta(q_0, a) = q_0,\ \delta(q_0, b) = q_0,\ \delta(q_0, c) = q_2,$$

$$\delta(q_1, a) = q_1,\ \delta(q_1, b) = q_0,\ \delta(q_1, c) = q_2,$$

$$\delta(q_2, a) = q_2,\ \delta(q_2, b) = q_1,\ \delta(q_2, c) = q_0,$$

e a função β definida por:

$$\beta(q_0, a) = 1,\ \beta(q_0, b) = 0,\ \beta(q_0, c) = 1,$$

$$\beta(q_1, a) = 1,\ \beta(q_1, b) = 0,\ \beta(q_1, c) = 1,$$

$$\beta(q_2, a) = 0,\ \beta(q_2, b) = 0,\ \beta(q_2, c) = 1.$$

A tabela de transições do autómato $\mathcal{M}$ é dada por:

δ	a	b	c
q_0	q_0	q_0	q_2
q_1	q_1	q_0	q_2
q_2	q_2	q_1	q_0

β	a	b	c
q_0	1	0	1
q_1	1	0	1
q_2	0	0	1

O diagrama de transições do autómato $\mathcal{M}$ é o apresentado na Figura 2.1.

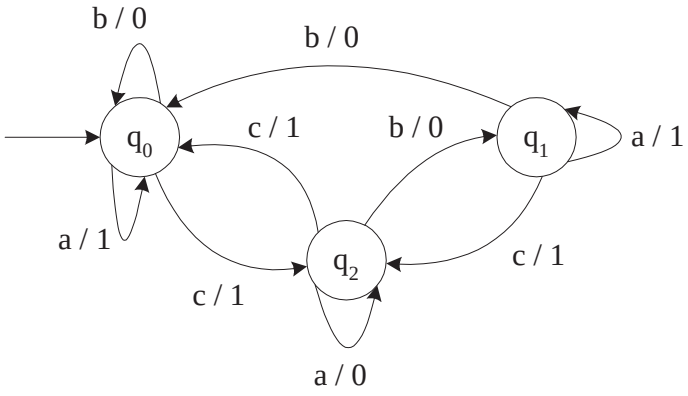


Figura 2.1: Diagrama de transições do autómato $\mathcal{M}$.

♢

Um dos objectivos desta tese é definir um autómato como uma álgebra heterogénea. Viu–se antes, que um autómato é definido como um sêxtuplo da forma $\mathcal{M} = (Z, I, O, \delta, \beta, z_0)$. Portanto, pode ser especificado pela assinatura $\Sigma_{aut} = \langle S, \Omega \rangle$ onde $S = \{\mathtt{z}, \mathtt{i}, \mathtt{o}\}$ e os símbolos de operação são: $\Omega_{\mathtt{zi},\mathtt{z}} = \{\delta\}$, $\Omega_{\mathtt{zi},\mathtt{o}} = \{\beta\}$, $\Omega_{\varepsilon,\mathtt{z}} = \{z_0\}$ e $\Omega_{w,a} = \emptyset$ para os outros casos. Assim, $\mathcal{M} = (M, \langle f^{\mathcal{M}} \rangle_{f \in \Omega})$ é a Σ_{aut}–álgebra, com $M = \langle Z, I, O \rangle$ e $\langle f^{\mathcal{M}} \rangle_{f \in \Omega} = \langle \delta, \beta, z_0 \rangle$. Como é usual utilizar–se–á a notação habitual para autómatos representado–os como sêxtuplos, listando primeiro os domínios e depois as operações.

Neste momento, tendo em conta esta definição algébrica de autómato, definir–se–á *autómato de Mealy* e só depois se definirá autómato de *Moore*, autómato finito determinístico e autómato finito não–determinístico.

Definição 2.2. Um *autómato de Mealy* é uma Σ_{aut}–álgebra $\mathcal{M} = (Z, I, O, \delta, \beta, z_0)$ onde:

– Z é um conjunto finito (não vazio) designado por *conjunto dos estados*;

– I é um conjunto finito (não vazio) designado por *alfabeto de input*;

– O é um conjunto finito (não vazio) designado por *alfabeto de output*.

A função $\delta : Z \times I \longrightarrow Z$ é designada por *função de transição de estados*, a função $\beta : Z \times I \longrightarrow O$ é a *função de outputs* e $z_0 \in Z$ é o *estado inicial* do autómato $\mathcal{M}$.

Exemplo 2.3. O autómato que se apresenta na Figura 2.2 é um autómato de *Mealy* definido por $\mathcal{M} = (Z, I, O, \delta, \beta, z_0)$, onde $Z = \{q_0, q_1, q_2\}$, $I = \{a, b\}$, $O = \{0, 1\}$, $z_0 = q_0$ e as funções δ e β são dadas pelo diagrama de transições.

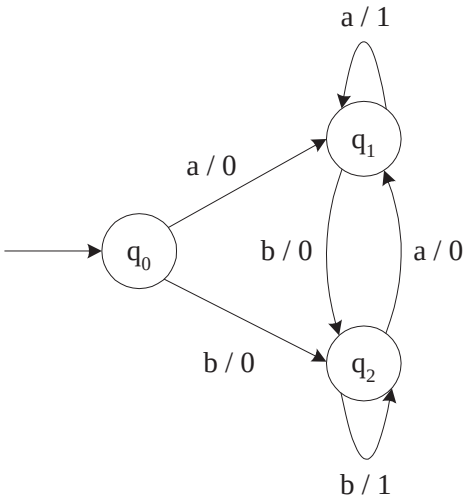


Figura 2.2: Diagrama de transições do autómato de *Mealy*.

♢

Num autómato de *Mealy* quando este se encontra no estado $z_0 \in Z$ e recebe a sequência de *inputs* $i_1 i_2 \ldots i_n \in I^*$ com $n \geq 0$, o autómato muda sucessivamente para os estados $z_1 = \delta(z_0, i_1)$, $z_2 = \delta(z_1, i_2), \ldots, z_n = \delta(z_{n-1}, i_n)$. Nestes autómatos o *output* está associado a cada transição de estado. Portanto, quando o autómato recebe a sequência de *inputs* $i_1 i_2 \ldots i_n \in I^*$, gera a sequência de *outputs* $\beta(z_0, i_1)$, $\beta(z_1, i_2), \ldots, \beta(z_n, i_n)$.

Quando um autómato de *Mealy* recebe como *input* a palavra vazia ε, o *output* gerado pelo autómato é a palavra vazia.

No Exemplo 2.3, se o autómato receber como sequência de *inputs* `abab`, a sequência de *outputs* que vai gerar é `0000`.

Seja $\mathcal{M} = (Z, I, O, \delta, \beta, z_0)$ um autómato de *Mealy*. Define–se de forma natural a *extensão* da função δ a I^*, $\delta^* : Z \times I^* \longrightarrow Z$, recursivamente do seguinte modo:

$$\begin{aligned} \delta^*(z, \varepsilon) &= z \\ \delta^*(z, aw) &= \delta^*(\delta(z, a), w), \end{aligned}$$

para quaisquer $z \in Z$, $a \in I$ e $w \in I^*$.

De igual modo, define–se a *extensão* da função β a I^*, $\beta^* : Z \times I^* \longrightarrow O^*$, recursivamente por:

$$\begin{aligned} \beta^*(z, \varepsilon) &= \varepsilon \\ \beta^*(z, aw) &= \beta(z, a) \cdot \beta^*(\delta(z, a), w), \end{aligned}$$

para quaisquer $z \in Z$, $a \in I$ e $w \in I^*$.

Os autómatos de *Moore* são semelhantes aos autómatos de *Mealy* com a diferença de terem os *outputs* associados aos estados.

De seguida, definir–se–á *autómato de Moore* como uma álgebra heterogénea.

Um autómato de *Moore* é um sêxtuplo da forma $\mathcal{M} = (Z, I, O, \delta, \lambda, z_0)$, com $\lambda : Z \longrightarrow O$. Portanto, pode ser especificado pela assinatura $\Sigma_{moo} = \langle S, \Omega \rangle$ onde $S = \{\mathtt{z}, \mathtt{i}, \mathtt{o}\}$ e os símbolos de operação são: $\Omega_{\mathtt{zi},\mathtt{z}} = \{\delta\}$, $\Omega_{\mathtt{z},\mathtt{o}} = \{\lambda\}$, $\Omega_{\varepsilon,\mathtt{z}} = \{z_0\}$ e $\Omega_{w,a} = \emptyset$ para os outros casos. Por conseguinte, $\mathcal{M} = (M, \langle f^{\mathcal{M}} \rangle_{f \in \Omega})$ é a Σ_{moo}–álgebra, com $M = \langle Z, I, O \rangle$ e $\langle f^{\mathcal{M}} \rangle_{f \in \Omega} = \langle \delta, \lambda, z_0 \rangle$. Como é usual utilizar–se–á a notação habitual para os autómatos, representando–os como um sêxtuplo, listando primeiro os domínios e depois as operações.

Definição 2.4. Um *autómato de Moore* é uma Σ_{moo}–álgebra $\mathcal{M} = (Z, I, O, \delta, \lambda, z_0)$ onde:

- Z é um conjunto finito (não vazio) designado por *conjunto dos estados*;
- I é um conjunto finito (não vazio) designado por *alfabeto de input*;
- O é um conjunto finito (não vazio) designado por *alfabeto de output*.

A função $\delta : Z \times I \longrightarrow Z$ é designada por *função de transição de estados*, $\lambda : Z \longrightarrow O$ é a *função de outputs* e $z_0 \in Z$ é o *estado inicial* do autómato $\mathcal{M}$.

Exemplo 2.5. O autómato que se apresenta na Figura 2.3 é o autómato de *Moore* definido por $\mathcal{M} = (Z, I, O, \delta, \lambda, z_0)$, onde $Z = \{q_0, q_1, q_2\}$, $I = \{0, 1\}$, $O = \{0, 1, m\}$, $z_0 = q_0$ e as funções δ e λ são dadas pelo diagrama de transições. ♢

A função de transição de estados de um autómato de *Moore* é igual à função de transição de estados de um autómato de *Mealy*. Como tal, o tipo de alterações que provocam no autómato são as mesmas. Mas, a função de *outputs* do autómato de *Moore* já actua de maneira diferente. Ou seja, o *output* nestes autómatos vai estar associado a cada estado, logo depende apenas do estado para que transita não dependendo do *input*. Assim, quando o autómato recebe a sequência de *inputs* $i_1 i_2 \ldots i_n \in I^*$ com $n \geq 0$, obtém–se a sequência de *outputs* $\lambda(z_0)$, $\lambda(z_1), \ldots, \lambda(z_n)$ onde $z_0, z_1, \ldots, z_n \in Z$ é a sequência de estados tais que, $\delta(z_{k-1}, i_k) = z_k$ para $k \in \{1, \ldots, n\}$.

Quando um autómato de *Moore* recebe como *input* a palavra vazia, o *output* gerado pelo autómato é $\lambda(z_0)$, ou seja é gerado o *output* correspondente ao estado inicial.

No Exemplo 2.5, o autómato recebe uma sequência de `0`'s e `1`'s e gera uma sequência de saída em que troca os `0`'s por `1`'s e os `1`'s por `0`'s. Se o autómato recebe ε, então o *output* gerado é `m`.

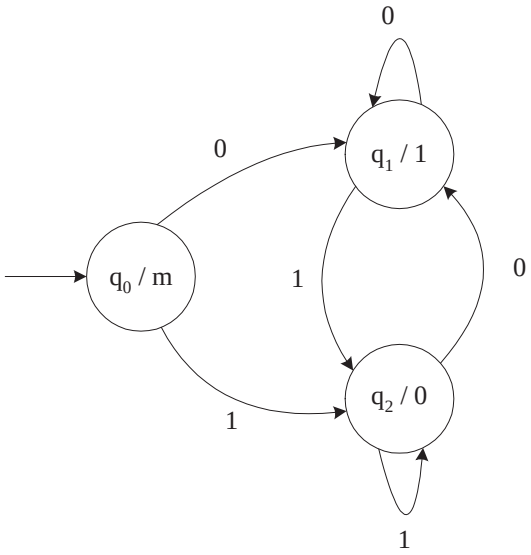


Figura 2.3: Diagrama de transições do autómato de *Moore*.

Seja $\mathcal{M}$ um autómato de *Moore*. A *extensão* da função δ a I^* do autómato de *Moore* define–se da mesma forma que a extensão da função δ a I^* do autómato de *Mealy*. Mas a extensão da função de *outputs* já é diferente. Define–se a *extensão* da função λ a I^*, $\lambda^* : Z \times I^* \longrightarrow O^*$, recursivamente por:

$$\lambda^*(z, \varepsilon) = \lambda(z)$$
$$\lambda^*(z, aw) = \lambda(z) \cdot \lambda^*(\delta(z, a), w),$$

para quaisquer $z \in Z$, $a \in I$ e $w \in I^*$.

Observe–se que os autómatos de *Mealy* e de *Moore* são autómatos muito semelhantes. Mas, uma diferença entre estes dois tipos de autómatos é a forma como geram o *output* correspondente à palavra vazia. Relembre–se que no caso do autómato de *Mealy*, quando este recebe como *input* a palavra vazia, o *output* gerado pelo autómato é a palavra vazia, enquanto que no caso do autómato de *Moore*, quando este recebe como *input* a palavra vazia, o *output* gerado pelo autómato é o *output* correspondente ao estado inicial do autómato. Mas, ultrapassando esta situação, consegue–se provar que um autómato de *Mealy* pode ser simulado por um autómato de *Moore*, e que um autómato de *Moore* pode ser simulado por um autómato de *Mealy*. Para tal, e em grosso modo, basta ignorar o *output* correspondente ao estado inicial no autómato de *Moore* e assim, verifica–se que existe uma equivalência entre os autómatos de *Mealy* e de *Moore*. Não se aprofundará este tema, uma vez que sai fora do âmbito desta tese, mas a prova poderá ser encontrada

em [7]. No entanto, de seguida, apresentar–se–á um exemplo da equivalência entre um autómato de *Mealy* e um autómato de *Moore*. Este exemplo foi retirado de [7].

A partir deste momento dar–se–á um maior relevo aos autómatos de *Mealy*.

Exemplo 2.6. Considere–se o autómato de *Mealy* que se apresenta na Figura 2.2. Neste exemplo constrói–se o autómato de *Moore* equivalente a esse autómato de *Mealy*. Este autómato de *Moore* é definido por $\mathcal{M} = (Z, I, O, \delta, \lambda, z_0)$ onde $Z = \{q_0/0, q_1/0, q_2/0, q_0/1, q_1/1, q_2/1\}$, $I = \{a, b\}$, $O = \{0, 1\}$, $z_0 = q_0/0$ e as transições e os *outputs* apresentam–se na Figura 2.4. Note-se que o estado $q_0/1$ podia ser removido, uma vez que nunca é alcançado.

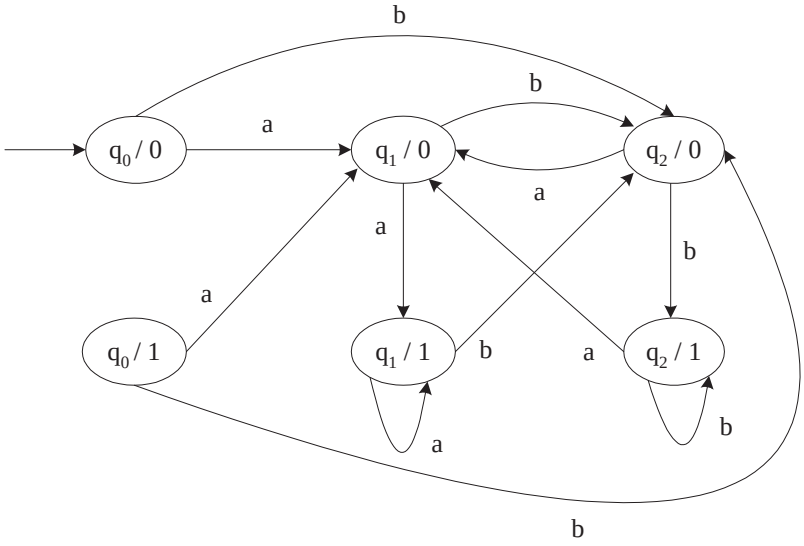


Figura 2.4: Diagrama de transições de um autómato de *Moore* equivalente ao autómato de *Mealy* da Figura 2.2.

♢

Neste momento, a partir da definição de autómato de *Mealy* definir–se–á autómato finito determinístico e finito não–determinístico.

Estes autómatos em relação aos autómatos de *Mealy* não têm alfabeto de *output*, nem função de *outputs*, mas têm um conjunto de estados finais ou de aceitação. Mais adiante, verificar–se–á que a partir de um autómato de *Mealy*, se pode obter um autómato finito determinístico.

Um autómato finito determinístico é um quíntuplo da forma $\mathcal{M} = (Z, I, \delta, z_0, F)$ onde Z é o *conjunto dos estados*, I é o *alfabeto de input*, $\delta : Z \times I \longrightarrow Z$ é a *função de transição*

de estados, $z_0 \in Z$ é o *estado inicial* do autómato e $F \subseteq Z$ é o *conjunto de estados finais* do autómato. Considere–se a assinatura $\Sigma_{AFD} = \langle S, \Omega \rangle$, onde $S = \{\mathtt{z}, \mathtt{i}\}$ e os símbolos de operação são: $\Omega_{\mathtt{zi},\mathtt{z}} = \{\delta\}$, $\Omega_{\varepsilon,\mathtt{z}} = \{z_0\}$ e $\Omega_{w,a} = \emptyset$ para os outros casos. Por conseguinte, a Σ_{AFD}–álgebra nesta assinatura é $\mathcal{A} = (A, \langle f^{\mathcal{A}} \rangle_{f \in \Omega})$ com, $A = \langle Z, I \rangle$ e $\langle f^{\mathcal{A}} \rangle_{f \in \Omega} = \langle \delta, z_0 \rangle$. Assim, define–se autómato finito determinístico, como um par constituído por esta álgebra nesta assinatura.

Definição 2.7. Um *autómato finito determinístico* é um par $\mathcal{M} = (\mathcal{A}, F)$ onde:

– $\mathcal{A}$ é uma Σ_{AFD}–álgebra, tal que Z e I são conjuntos finitos (não vazios);

– $F \subseteq Z$.

Como é usual utilizar–se–á a notação habitual para autómatos, representando–os como um quíntuplo, listando primeiro os domínios, depois as operações e só depois o conjunto F.

Exemplo 2.8. O autómato que se apresenta na Figura 2.5 é o autómato finito determinístico $\mathcal{M} = (Z, I, \delta, z_0, F)$, onde $Z = \{q_0, q_1, q_2\}$, $I = \{0, 1\}$, $z_0 = q_0$, $F = \{q_1\}$ e δ é dada pelo diagrama de transições.

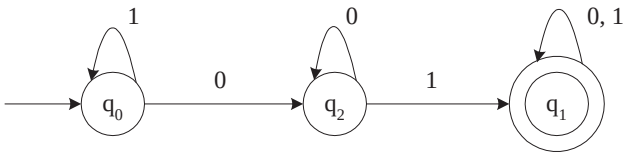


Figura 2.5: Diagrama de transições de $\mathcal{M}$.

♢

Também para estes autómatos se pode estender a função de transição de estados a I^*, sendo esta definida da mesma forma que a extensão da função δ do autómato de *Mealy*.

Os autómatos finitos determinísticos podem actuar como reconhecedores (ou aceitadores) de linguagens. A linguagem *aceite* ou *reconhecida* por um autómato finito determinístico $\mathcal{M} = (Z, I, \delta, z_0, F)$ é a linguagem:

$$L(\mathcal{M}) = \{w \in I^* : \delta^*(z_0, w) \in F\}.$$

De modo informal, diz–se que a linguagem aceite ou reconhecida por um autómato finito determinístico, consiste no conjunto de sequências de símbolos, que no diagrama de transições, correspondem a caminhos desde o estado inicial até um dos estados finais.

Portanto, o autómato apresentado no Exemplo 2.8 aceita ou reconhece palavras em que a sequência `01` está "contida". Portanto, a linguagem que o autómato aceita ou reconhece é: $L(\mathcal{M}) = \{w \in I^* \ : \ \text{a sequência } \texttt{01} \text{ é parte de } w\}$.

Introduz–se agora a definição de *linguagem racional*.

Definição 2.9. Seja A um alfabeto. O *conjunto das linguagens racionais* sobre A é o menor conjunto de linguagens que, satisfaz as seguintes condições:

- Se $L \subseteq A^*$ é uma linguagem finita então L é uma linguagem racional;
- Se $L_1, L_2 \subseteq A^*$ são linguagens racionais então $L_1 \cup L_2$ é uma linguagem racional;
- Se $L_1, L_2 \subseteq A^*$ são linguagens racionais então $L_1 L_2$ é uma linguagem racional;
- Se $L \subseteq A^*$ é uma linguagem racional então L^* é uma linguagem racional.

Um resultado importante em que é relevante a importância desta definição é o *Teorema de Kleene*, que pode ser encontrado em [2] e [8] com a respectiva prova. Este teorema afirma que, uma dada linguagem é aceite ou reconhecida por um autómato finito determinístico se e só se essa linguagem for racional.

Autómatos finitos não–determinísticos vs autómatos finitos determinísticos

Neste momento, definir–se–á *autómato finito não–determinístico*. Este tipo de autómatos em relação aos autómatos finitos determinísticos tem uma função de transição de estados diferente. Assim, será dada uma ideia de como esta actua e apresentar–se–á um exemplo. Para além disso, constatar–se–á que para todo o autómato finito não–determinístico se pode construir um autómato finito determinístico equivalente.

Definição 2.10. Um *autómato finito não–determinístico* é um quíntuplo da forma $\mathcal{M} = (Z, I, \delta, z_0, F)$ onde:

- Z é um conjunto finito (não vazio) designado por *conjunto dos estados*;
- I é um conjunto finito (não vazio) designado por *alfabeto de input*.

A função $\delta : Z \times I \longrightarrow \mathcal{P}(Z)$ é a *função de transição de estados*, onde $\mathcal{P}(Z)$ denota o conjunto de todos os subconjuntos de Z, $z_0 \in Z$ é o *estado inicial* do autómato $\mathcal{M}$ e $F \subseteq Z$ é o *conjunto de estados finais* do autómato $\mathcal{M}$.

Observe–se que δ não é uma função simples, não sendo portanto vantajoso transformar o autómato finito não–determinístico numa álgebra. Mais à frente, perceber–se–á que não é necessário, dado que estes autómatos se podem reduzir a autómatos finitos determinísticos.

Exemplo 2.11. O autómato que se apresenta na Figura 2.6 é um autómato finito não–determinístico definido por $\mathcal{M} = (Z, I, \delta, z_0, F)$, onde $Z = \{q_0, q_1, q_2, q_3, q_4, q_5, q_6\}$, $I = \{0, 1\}$, $z_0 = q_0$, $F = \{q_3, q_6\}$ e a função δ é dada pelo diagrama de transições.

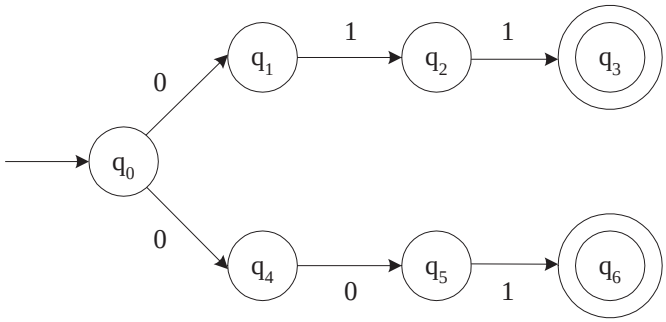


Figura 2.6: Diagrama de transições de $\mathcal{M}$.

$\diamondsuit$

Os autómatos finitos determinísticos e os autómatos finitos não–determinísticos, diferem na função de transição de estados δ, a qual no caso dos autómatos finitos não–determinísticos está definida de $Z \times I$ para $\mathcal{P}(Z)$. De um modo informal, isto quer dizer que um *input* não determina um e um único próximo estado. A função de transição de estados pode ser *indefinida* e nesse caso $\delta(z, i) = \emptyset$, para algum $z \in Z$ e $i \in I$, ou pode ser *ambígua* e nesse caso $\delta(z, i)$ contém mais do que um elemento de Z, para algum $z \in Z$ e $i \in I$. No Exemplo 2.11 verifica–se que δ é indefinida, por exemplo em $\delta(q_1, 0) = \delta(q_2, 0) = \delta(q_3, 0) = \delta(q_5, 0) = \delta(q_6, 0) = \emptyset$ e que δ é ambígua, por exemplo em $\delta(q_0, 0) = \{q_1, q_4\}$.

Seja $\mathcal{M}$ um autómato finito não–determinístico. Define–se de forma natural a *extensão* da função δ^* a I^*, $\delta^* : Z \times I^* \longrightarrow \mathcal{P}(Z)$, recursivamente por:

$$\begin{aligned} \delta^*(z, \varepsilon) &= \{z\} \\ \delta^*(z, aw) &= \bigcup_{p \in \delta(z,a)} \delta^*(p, w), \end{aligned}$$

para quaisquer $z \in Z$, $a \in I$ e $w \in I^*$.

Os autómatos finitos não–determinísticos são autómatos que também reconhecem linguagens. Neste caso, um autómato $\mathcal{M} = (Z, I, \delta, z_0, F)$ *aceita* ou *reconhece* a linguagem:

$$L(\mathcal{M}) = \{w \in I^* : \delta^*(z_0, w) \cap F \neq \emptyset\}.$$

No Exemplo 2.11, a linguagem aceite ou reconhecida pelo autómato apresentado é $L(\mathcal{M}) = \{01^2,\ 0^21\}$.

Um autómato finito determinístico é um caso especial de um autómato finito não–determinístico, onde para cada estado existe uma única transição para cada *input*. Deste modo, num autómato finito determinístico, para uma determinada palavra $w \in I^*$ e um determinado estado $z \in Z$, existe exactamente um caminho que se encontra rotulado para w e que começa em z. Portanto, para determinar se uma palavra w é aceite ou reconhecida por um autómato finito determinístico, basta verificar se existe um caminho rotulado para w que começa no estado inicial e termina num estado final. Num autómato finito não–determinístico podem haver muitos caminhos rotulados para a palavra $w \in I^*$ e deve–se testar se pelo menos um termina num estado final. Assim, qualquer linguagem reconhecida por um autómato finito determinístico pode também ser reconhecida por um autómato finito não–determinístico. O que não é tão óbvio é que os autómatos finitos não–determinísticos reconhecem as mesmas linguagens que os autómatos finitos determinísticos.

Para provar este facto, basta mostrar que para todo o autómato finito não–determinístico se pode construir um autómato finito determinístico equivalente, ou seja que reconhece a mesma linguagem. Como esta equivalência se encontra fora do âmbito desta tese, apresentar–se–á apenas um exemplo. A prova dessa equivalência pode ser encontrada em [7].

Exemplo 2.12. Seja $\mathcal{M} = (Z, I, \delta, z_0, F)$, com $Z = \{q_0, q_1, q_2\}$, $I = \{0, 1\}$, $z_0 = q_0$ e $F = \{q_2\}$ um autómato finito não–determinístico, que reconhece as cadeias binárias que terminam em `01` e cujo diagrama de transição se apresenta na Figura 2.7. O autómato finito determinístico equivalente apresenta–se na Figura 2.8.

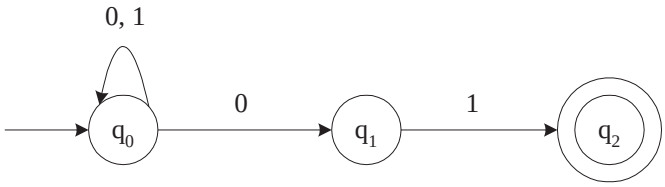


Figura 2.7: Diagrama de transições do autómato finito não–determinístico $\mathcal{M}$.

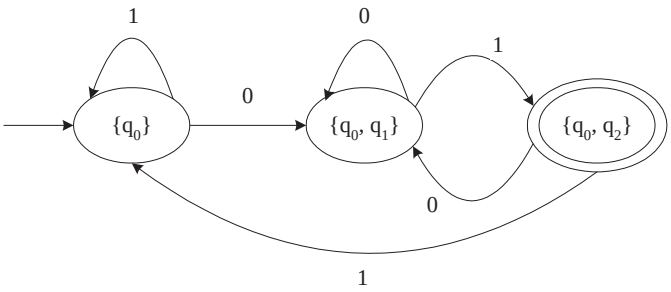


Figura 2.8: Diagrama de transições do autómato finito determinístico equivalente ao autómato finito não–determinístico $\mathcal{M}$.

♢

Autómatos finitos determinísticos vs autómatos de *Mealy*

Como já foi referido anteriormente, os autómatos finitos determinísticos e os autómatos de *Mealy* não são estruturas na mesma assinatura, no entanto a partir de um autómato finito determinístico pode–se construir um autómato de *Mealy*, que reproduz, em certo sentido, o comportamento do autómato finito determinístico.

Seja $\mathcal{M} = (Z, I, \delta, z_0, F)$ um autómato finito determinístico. Como foi visto antes uma determinada palavra $w \in I^*$ é aceite ou reconhecida pelo autómato $\mathcal{M}$ se e só se $\delta^*(z_0, w) \in F$. Considere–se agora o autómato de *Mealy* $\mathcal{N} = (Z, I, O, \delta, \beta, z_0)$ construído a partir de $\mathcal{M}$, onde $O = \{0, 1\}$ e $\beta : Z \times I \longrightarrow O$ é definida por:

$$\beta(z, i) = \begin{cases} 1 \text{ se } \delta(z, i) \in F \\ 0 \text{ se } \delta(z, i) \notin F \end{cases} \tag{2.1}$$

Pode–se definir palavra e linguagem aceite por um autómato de *Mealy*. Diz–se que, $w \in I^*$ é aceite por $\mathcal{N}$ se e só se, $\beta^*(z_0, w) \in \{0, 1\}^*1 \cup \{\varepsilon\}$ e $z_0 \in F$ ou $\beta^*(z_0, w) \in \{0, 1\}^*1$ e $z_0 \notin F$. O conjunto de todas as palavras aceites por $\mathcal{N}$ designa–se por *linguagem aceite por* $\mathcal{N}$ e denota–se por $L(\mathcal{N})$. Prova–se facilmente que uma palavra é aceite por $\mathcal{N}$ se e só se é aceite por $\mathcal{M}$. Logo, $\mathcal{M}$ e $\mathcal{N}$ aceitam a mesma linguagem. Assim, conclui–se que qualquer autómato finito determinístico é equivalente a um autómato de *Mealy*, onde a função β é definida como em (2.1). Um exemplo ilustrará melhor esta equivalência.

Exemplo 2.13. Seja $\mathcal{M} = (Z, I, \delta, z_0, F)$ um autómato finito determinístico onde $Z = \{q_0, q_1, q_2\}$, $I = \{a, b\}$, $z_0 = q_0$, $F = \{q_1\}$ e δ é dada pelo diagrama de transições da Figura 2.9. A Figura 2.10 mostra as transições e os *outputs* do autómato de *Mealy* $\mathcal{N} = (Z, I, O, \delta, \beta, z_0)$ equivalente a $\mathcal{M}$. ♢

Portanto, dado um autómato finito determinístico $\mathcal{M}$, pode–se obter facilmente um

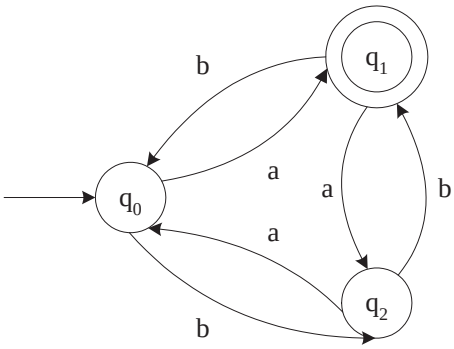


Figura 2.9: Diagrama de transições do autómato $\mathcal{M}$.

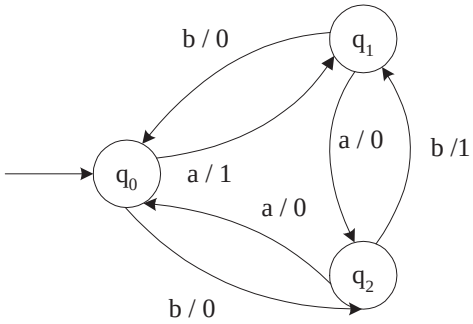


Figura 2.10: Diagrama de transições do autómato $\mathcal{N}$.

autómato de *Mealy* que reconhece a mesma linguagem que $\mathcal{M}$. Daqui por diante, de forma a criar uma maior generalidade nas definições e resultados a apresentar, o tipo de autómatos que se utilizará são os autómatos de *Mealy*.

2 Homomorfismos e isomorfismos entre autómatos

No Capítulo 1 apresentou–se a definição de homomorfismo e isomorfismo, para álgebras heterogéneas e na secção anterior, definiu–se autómato de *Mealy* como uma álgebra heterogénea. Portanto, as definições de homomorfismo e isomorfismo apresentadas, aplicam–se em particular para os autómatos de *Mealy*.

Em seguida, ir–se–á instanciar para a assinatura Σ_{aut} as definições de homomorfismo e isomorfismo apresentadas no Capítulo 1 para as assinaturas gerais.

Sejam $\mathcal{M}_1 = (Z_1, I_1, O_1, \delta_1, \beta_1, z_1)$ e $\mathcal{M}_2 = (Z_2, I_2, O_2, \delta_2, \beta_2, z_2)$ Σ_{aut}–álgebras.

Uma função Φ de M_1 para M_2 tem três componentes, nomeadamente a componente

$\alpha : Z_1 \longrightarrow Z_2$, a componente $\tau : I_1 \longrightarrow I_2$ e a componente $\theta : O_1 \longrightarrow O_2$. Em seguida, representar–se–á Φ como o terno $\Phi = (\alpha, \tau, \theta)$.

Não é difícil verificar que Φ é um *homomorfismo* de $\mathcal{M}_1$ para $\mathcal{M}_2$ se e só se para todo o $z \in Z_1$ e $i \in I_1$,

$$\alpha(\delta_1(z, i)) = \delta_2(\alpha(z), \tau(i)) \tag{2.2}$$

$$\theta(\beta_1(z, i)) = \beta_2(\alpha(z), \tau(i)) \tag{2.3}$$

$$\alpha(z_1) = z_2. \tag{2.4}$$

De seguida, mostrar–se–á que as condições (2.2) e (2.3) se verificam para as suas extensões. Para tal, será necessário introduzir a definição que se segue.

Sejam A e B conjuntos e $f : A \longrightarrow B$ uma função. Define–se recursivamente $f^* : A^* \longrightarrow B^*$ por:

1. $f^*(\varepsilon) = \varepsilon$;
2. $f^*(aw) = f(a) \cdot f^*(w)$, com $a \in A$ e $w \in A^*$.

Lema 2.14. *Sejam $\mathcal{M}_1 = (Z_1, I_1, O_1, \delta_1, \beta_1, z_1)$ e $\mathcal{M}_2 = (Z_2, I_2, O_2, \delta_2, \beta_2, z_2)$ Σ_{aut}–álgebras e seja $\Phi = (\alpha, \tau, \theta)$ um homomorfismo de $\mathcal{M}_1$ para $\mathcal{M}_2$. Então, para todo o $z \in Z_1$ e $w \in I_1^*$*

$$\alpha(\delta_1^*(z, w)) = \delta_2^*(\alpha(z), \tau^*(w)), \tag{2.5}$$

$$\theta^*(\beta_1^*(z, w)) = \beta_2^*(\alpha(z), \tau^*(w)). \tag{2.6}$$

Demonstração. A demonstração deste Lema será efectuada por indução sobre o comprimento da palavra $w \in I_1^*$.

Inicia–se a demonstração começando por mostrar a condição (2.5). Se $|w| = 0$ então $w = \varepsilon$ e portanto,

$$\alpha(\delta_1^*(z, \varepsilon)) = \alpha(z), \text{ por definição de } \delta_1^*.$$

e

$$\begin{aligned} \delta_2^*(\alpha(z), \tau^*(\varepsilon)) &= \delta_2^*(\alpha(z), \varepsilon), \text{ por definição de } \tau^* \\ &= \alpha(z), \text{ por definição de } \delta_2^*. \end{aligned}$$

Logo, a condição (2.5) verifica–se quando $|w| = 0$.

Suponha–se agora que $w' = iw$, com $i \in I_1$ e $w \in I_1^*$ e suponha–se que,

$$\alpha(\delta_1^*(z, w)) = \delta_2^*(\alpha(z), \tau^*(w)).$$

Pretende–se provar que:

$$\alpha(\delta_1^*(z, iw)) = \delta_2^*(\alpha(z), \tau^*(iw)).$$

Assim,

$$\begin{aligned}\delta_2^*(\alpha(z),\tau^*(iw)) &= \delta_2^*(\alpha(z),\tau(i)\cdot\tau^*(w)),\ \text{por definição de } \tau^*\\ &= \delta_2^*(\delta_2(\alpha(z),\tau(i)),\tau^*(w)),\ \text{por definição de } \delta_2^*\\ &= \delta_2^*(\alpha(\delta_1(z,i)),\tau^*(w)),\ \text{pois } \Phi \text{ é um homomorfismo}\\ &= \alpha(\delta_1^*(\delta_1(z,i),w)),\ \text{por hipótese de indução}\\ &= \alpha(\delta_1^*(z,iw)),\ \text{por definição de } \delta_1^*.\end{aligned}$$

Logo, a condição (2.5) verifica–se para $w' = iw$.

Mostra–se agora a condição (2.6).

Se $|w| = 0$ então $w = \varepsilon$ e portanto,

$$\begin{aligned}\theta^*(\beta_1^*(z,\varepsilon)) &= \theta^*(\varepsilon),\ \text{por definição de } \beta_1^*\\ &= \varepsilon,\ \text{por definição de } \theta^*.\end{aligned}$$

e

$$\begin{aligned}\beta_2^*(\alpha(z),\tau^*(\varepsilon)) &= \beta_2^*(\alpha(z),\varepsilon),\ \text{por definição de } \tau^*\\ &= \varepsilon,\ \text{por definição de } \beta_2^*.\end{aligned}$$

Logo, a condição (2.6) verifica–se quando $|w| = 0$.

Suponha–se agora que $w' = iw$, com $i \in I_1$ e $w \in I_1^*$ e suponha–se que,

$$\theta^*(\beta_1^*(z,w)) = \beta_2^*(\alpha(z),\tau^*(w)).$$

Pretende–se provar que:

$$\theta^*(\beta_1^*(z,iw)) = \beta_2^*(\alpha(z),\tau^*(iw)).$$

Assim,

$$\begin{aligned}\beta_2^*(\alpha(z),\tau^*(iw)) &= \beta_2^*(\alpha(z),\tau(i)\cdot\tau^*(w)),\ \text{por definição de } \tau^*\\ &= \beta_2(\alpha(z),\tau(i))\cdot\beta_2^*(\delta_2(\alpha(z),\tau(i)),\tau^*(w)),\ \text{por definição de } \beta_2^*\\ &= \theta(\beta_1(z,i))\cdot\beta_2^*(\alpha(\delta_1(z,i)),\tau^*(w)) \text{ pois } \Phi \text{ é um homomorfismo}\\ &= \theta(\beta_1(z,i))\cdot\theta^*(\beta_1^*(\delta_1(z,i),w)),\ \text{por hipótese de indução}\\ &= \theta^*(\beta_1(z,i)\cdot\beta_1^*(\delta_1(z,i),w)),\ \text{por definição de } \theta^*\\ &= \theta^*(\beta_1^*(z,iw)),\ \text{por definição de } \beta_1^*.\end{aligned}$$

Logo, a condição (2.6) verifica–se para $w' = iw$. E fica assim provado o Lema.

□

Exemplo 2.15. Considere–se o autómato de *Mealy* $\mathcal{M}_1 = (Z_1, I_1, O_1, \delta_1, \beta_1, z_1)$ com, $Z_1 = \{q_0, q_1, q_2\}$, $I_1 = \{a, b\}$, $O_1 = \{x, y, z\}$, $z_1 = q_0$ e as funções δ_1 e β_1 são dadas pelo diagrama de transições que se apresenta na Figura 2.11.

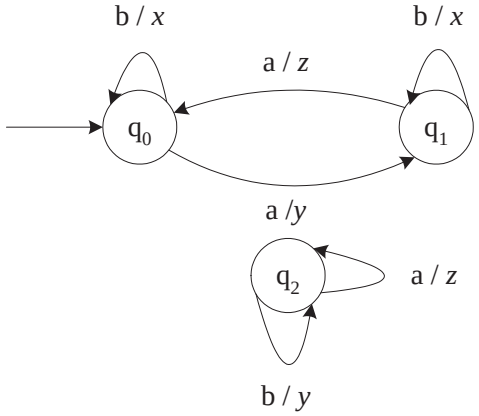


Figura 2.11: Diagrama de transições do autómato $\mathcal{M}_1$.

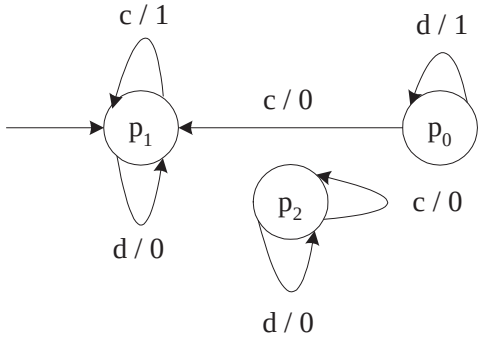


Figura 2.12: Diagrama de transições do autómato $\mathcal{M}_2$.

E considere–se $\mathcal{M}_2 = (Z_2, I_2, O_2, \delta_2, \beta_2, z_2)$ também um autómato de *Mealy*, onde $Z_2 = \{p_0, p_1, p_2\}$, $I_2 = \{c, d\}$, $O_2 = \{0, 1\}$, $z_2 = p_1$ e as funções δ_2 e β_2 são dadas pelo diagrama de transições que se apresenta na Figura 2.12.

A aplicação $\Phi = (\alpha, \tau, \theta)$ com $\alpha(q_0) = \alpha(q_1) = p_1$, $\alpha(q_2) = p_2$, $\tau(a) = d$, $\tau(b) = c$ e $\theta(x) = 1$, $\theta(y) = \theta(z) = 0$ é um homomorfismo do autómato $\mathcal{M}_1$ para o autómato $\mathcal{M}_2$.

$\diamondsuit$

A par do que se viu no Capítulo 1, Φ é um *isomorfismo* de $\mathcal{M}_1$ para $\mathcal{M}_2$, se Φ é um homomorfismo e as funções α, τ e θ são bijectivas. Quando tal isomorfismo existe, diz–se que as Σ_{aut}–álgebras $\mathcal{M}_1$ e $\mathcal{M}_2$ são *isomorfas*, e escreve–se: $\mathcal{M}_1 \cong \mathcal{M}_2$.

Note–se que, $\Phi^{-1} = (\alpha^{-1}, \tau^{-1}, \theta^{-1})$ é o *isomorfismo inverso* de Φ, se as componentes são definidas por: $\alpha^{-1} : Z_2 \longrightarrow Z_1$, $\tau^{-1} : I_2 \longrightarrow I_1$ e $\theta^{-1} : O_2 \longrightarrow O_1$. Por sua vez, sendo

$\mathcal{M} = (Z, I, O, \delta, \beta, z_0)$ uma Σ_{aut}–álgebra, o *isomorfismo identidade* de $\mathcal{M}$, que se denota por $Id_{\mathcal{M}}$, é o isomorfismo com as componentes α, τ e θ funções identidade.

Tendo por base a definição de homomorfismo apresentada, define–se agora *homomorfismo de redução*.

Definição 2.16. Sejam $\mathcal{M}_1 = (Z_1, I_1, O_1, \delta_1, \beta_1, z_1)$ e $\mathcal{M}_2 = (Z_2, I_2, O_2, \delta_2, \beta_2, z_2)$ Σ_{aut}–álgebras. E seja $\Phi = (\alpha, \tau, \theta)$ um homomorfismo de $\mathcal{M}_1$ para $\mathcal{M}_2$. Diz–se que Φ é um *homomorfismo de redução*, ou é uma *redução*, se:

1. α é sobrejectiva;

2. $I_1 = I_2$ e τ é a função identidade;

3. $O_1 = O_2$ e θ é a função identidade.

Exemplo 2.17. [11] Considere–se o autómato de *Mealy* $\mathcal{M}_1 = (Z_1, I_1, O_1, \delta_1, \beta_1, z_1)$, onde $Z_1 = \{q_0, q_1, q_2, q_3\}$, $I_1 = \{a, b\}$, $O_1 = \{0, 1\}$, $z_1 = q_0$ e as funções δ_1 e β_1 são dadas pelo diagrama de transições que se apresenta na Figura 2.13. E considere–se $\mathcal{M}_2 = (Z_2, I_2, O_2, \delta_2, \beta_2, z_2)$ também um autómato de *Mealy*, onde $Z_2 = \{p_0, p_1, p_2\}$, $I_2 = \{a, b\}$, $O_2 = \{0, 1\}$, $z_2 = p_0$ e as funções δ_2 e β_2 são dadas pelo diagrama de transições que se apresenta na Figura 2.14. Facilmente se verifica, que a aplicação $\Phi = (\alpha, \tau, \theta)$ com $\alpha(q_0) = \alpha(q_1) = p_0$, $\alpha(q_2) = p_1$, $\alpha(q_3) = p_2$, $\tau(a) = a$, $\tau(b) = b$ e $\theta(0) = 0$, $\theta(1) = 1$ é um homomorfismo do autómato $\mathcal{M}_1$ para o autómato $\mathcal{M}_2$. Como α é sobrejectiva e τ e θ são funções identidade então Φ é um homomorfismo de redução.

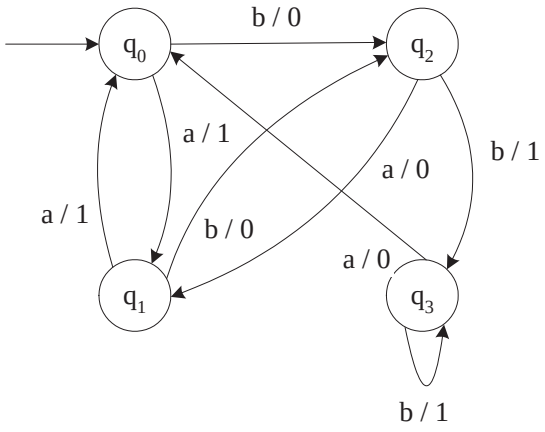


Figura 2.13: Diagrama de transições de $\mathcal{M}_1$.

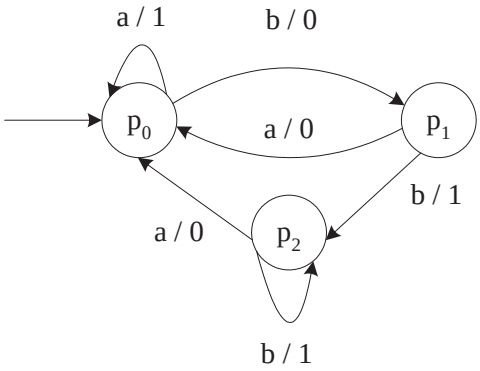


Figura 2.14: Diagrama de transições de $\mathcal{M}_2$.

$\diamondsuit$

3 Congruências e autómato quociente

Inicia–se esta secção definindo partição para um autómato.

Seja $\mathcal{M} = (Z, I, O, \delta, \beta, z_0)$ um autómato de *Mealy*. Uma *partição* π do conjunto de estados do autómato $\mathcal{M}$ é um conjunto de subconjuntos de Z, tais que todo o elemento de Z pertence exactamente a um desses subconjuntos.

Esta partição π induz uma relação de equivalência $R_\pi \subseteq Z \times Z$, que se pode estender a uma S–relação de equivalência da forma $\Theta(\pi) = (R_\pi, R_I, R_O)$, onde R_I é a relação diagonal no alfabeto de *input* e R_O é a relação diagonal no alfabeto de *output*.

Na literatura tradicional sobre autómatos [11], algumas das condições que se irão apresentar, são dadas para a partição π e não para a relação $\Theta(\pi)$. Portanto, no que se segue no texto trabalhar–se–á com partições, no entanto sempre que seja oportuno efectuar–se–á referência a $\Theta(\pi)$, no sentido em que algumas propriedades requeridas à partição π, do conjunto de estados Z, traduzem–se em propriedades da relação de equivalência R_π, como se perceberá de seguida.

Considere–se $\mathcal{M}_1 = (Z_1, I_1, O_1, \delta_1, \beta_1, z_1)$ e $\mathcal{M}_2 = (Z_2, I_2, O_2, \delta_2, \beta_2, z_2)$ Σ_{aut}–álgebras. Suponha–se que $\Phi = (\alpha, \tau, \theta)$ é um homomorfismo de redução entre $\mathcal{M}_1$ e $\mathcal{M}_2$. A função α é sobrejectiva, e portanto determina uma partição de Z_1, cujos blocos se encontram numa correspondência injectiva com os elementos de Z_2. Pode–se deste modo construir uma cópia de $\mathcal{M}_2$, utilizando os blocos dessa partição como estados. Isto é, para cada $y \in Z_2$ vai existir um conjunto $\alpha^{-1}(y)$, que é o conjunto de todos os estados de Z_1 que são transformados em $y \in Z_2$ por α. Esses conjuntos formam uma partição de Z_1, que se designará por π_α.

Assim, pode–se construir uma Σ_{aut}–álgebra isomorfa a $\mathcal{M}_2$ cuja existência é garantida pelo Primeiro Teorema do Homomorfismo. Essa Σ_{aut}–álgebra obtém–se substituindo cada $y \in Z_2$ por $\alpha^{-1}(y)$. Logo, é definida por:

$$\mathcal{M}' = (\pi_\alpha, I_1, O_1, \delta', \beta', z_1),$$

onde, para $i \in I_1 = I_2$ e $x \in Z_2$ vem que:

$$\delta'(\alpha^{-1}(x), i) = \alpha^{-1}(\delta_2(x, i)) \tag{2.7}$$

$$\beta'(\alpha^{-1}(\delta_2(x, i)), i) = \beta_2(\delta_2(x, i), i) \tag{2.8}$$

Facilmente se verifica que as funções δ' e β' estão bem definidas.

Exemplo 2.18. Com as condições referidas no Exemplo 2.17, pode–se verificar que: $\alpha^{-1}(p_0) = \{q_0, q_1\}$, $\alpha^{-1}(p_1) = \{q_2\}$ e $\alpha^{-1}(p_2) = \{q_3\}$. Assim, uma partição de Z_1 é $\pi_1 = \Big\{\{q_0, q_1\}, \{q_2\}, \{q_3\}\Big\}$. Esta partição é o conjunto de estados do autómato $\mathcal{M}'$, cujo diagrama de transições é o apresentado na Figura 2.15.

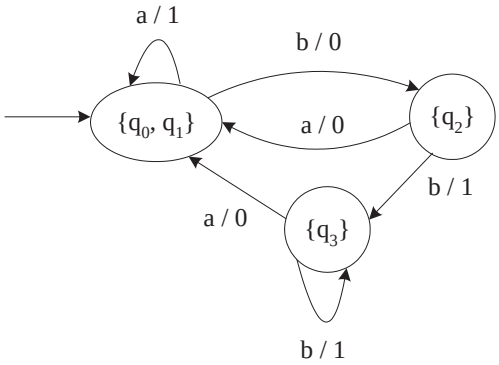


Figura 2.15: Diagrama de transições do autómato $\mathcal{M}'$.

♢

Introduz–se de seguida a seguinte definição:

Definição 2.19. Seja $\mathcal{M} = (Z, I, O, \delta, \beta, z_0)$ uma Σ_{aut}–álgebra e sejam $X \subseteq Z$ e $i \in I$. Define–se:

1. $\delta(X, i) = \{\delta(x, i) \ : \ x \in X\}$,
2. $\beta(X, i) = \{\beta(x, i) \ : \ x \in X\}$

Lema 2.20. *Sejam* $\mathcal{M}_1 = (Z_1, I_1, O_1, \delta_1, \beta_1, z_1)$ *e* $\mathcal{M}_2 = (Z_2, I_2, O_2, \delta_2, \beta_2, z_2)$ Σ_{aut}*–álgebras e seja* $\Phi = (\alpha, \tau, \theta)$ *um homomorfismo de redução entre* $\mathcal{M}_1$ *e* $\mathcal{M}_2$*. Seja* $\mathcal{M}' = (\pi_\alpha, I_1, O_1, \delta', \beta', z_1)$ *a* Σ_{aut}*–álgebra isomorfa a* $\mathcal{M}_2$*. Então, para todo* $X, X' \in \pi_\alpha$*,* $i \in I_1$ *e* $o \in O_1$*, vem que:*

1. $\delta'(X, i) = X' \Rightarrow \delta_1(X, i) \subseteq X'$
2. $\beta'(X, i) = \{o\} \Rightarrow \beta_1(X, i) = \{o\}$

e portanto,

3. *para todo o* $X \in \pi_\alpha$ *e* $i \in I_1$*, existe* $X' \in \pi_\alpha$ *e* $o \in O_1$*, tal que* $\delta_1(X, i) \subseteq X'$ *e* $\beta_1(X, i) = \{o\}$*.*

Demonstração. Começa–se por provar a condição 1. do Lema. Suponha–se que $X, X' \in \pi_\alpha$, $i \in I_1 = I_2$ e $\delta'(X, i) = X'$. Dado que $X, X' \in \pi_\alpha$ então existem $y, y' \in Z_2$ tais que:

$$X = \alpha^{-1}(y) \quad \text{e} \quad X' = \alpha^{-1}(y') \tag{2.9}$$

Assim,

$$\begin{aligned} \delta'(X, i) &= \delta'(\alpha^{-1}(y), i), \text{ por (2.9)} \\ &= \alpha^{-1}(\delta_2(y, i)), \text{ por (2.7)}. \end{aligned}$$

Por outro lado,

$$\begin{aligned} \delta'(X, i) &= X', \\ &= \alpha^{-1}(y'), \text{ por (2.9)}. \end{aligned}$$

Então, $\alpha^{-1}(\delta_2(y, i)) = \alpha^{-1}(y')$. Assim, por definição de π_α,

$$\delta_2(y, i) = y'. \tag{2.10}$$

Suponha–se que $x \in X$ e seja $\delta_1(x, i) = x'$. Sabe–se por (2.9) que $X = \alpha^{-1}(y)$ então para $x \in X$, $\alpha(x) = y$. Deste modo,

$$\begin{aligned} \delta_2(y, i) &= \delta_2(\alpha(x), i), \\ &= \alpha(\delta_1(x, i)), \text{ pois } \Phi \text{ é um homomorfismo de redução.} \end{aligned}$$

Mas, por (2.10) $\delta_2(y, i) = y'$. Então conclui–se que

$$\begin{aligned} y' &= \alpha(\delta_1(x, i)), \\ &= \alpha(x'), \text{ pois } \delta_1(x, i) = x'. \end{aligned}$$

E daqui conclui–se que $x' = \alpha^{-1}(y')$. Como por (2.9) $X' = \alpha^{-1}(y')$ então $x' \in X'$. Por outro lado $x' = \delta_1(x, i)$ então $\delta_1(x, i) \in X'$. E portanto, $\delta_1(X, i) \subseteq X'$.

Prova–se agora a condição 2. do Lema. Suponha–se que $X \in \pi_\alpha$, $o \in O_1 = O_2$ e $\beta'(X,i) = \{o\}$. Como $X \in \pi_\alpha$, então por definição de π_α, existe $y \in Z_2$ tal que

$$X = \alpha^{-1}(y) \tag{2.11}$$

Assim,

$$\begin{aligned}\beta'(X,i) &= \beta'(\alpha^{-1}(y),i), \text{ por (2.11)}\\ &= \beta_2(y,i), \text{ por (2.8)}.\end{aligned}$$

Por outro lado, $\beta'(X,i) = \{o\}$, como tal $\beta_2(y,i) = o$.

Suponha–se agora que $x \in X$. Como $X = \alpha^{-1}(y)$ então $\alpha(x) = y$. Portanto,

$$\begin{aligned}\beta_2(y,i) &= \beta_2(\alpha(x),i),\\ &= \beta_1(x,i), \text{ pois } \Phi \text{ é um homomorfismo de redução.}\end{aligned}$$

.

Como $\beta_2(y,i) = o$ então vem que $\beta_1(x,i) = o$. Portanto, $\beta_1(X,i) = \{o\}$.

Falta provar a condição 3. do Lema. Para isso, basta tomar $X' = \delta'(X,i)$ e $\{o\} = \beta'(X,i)$ e a prova reduz-se às provas de 1. e 2. que se efectuou anteriormente. □

Deste modo, concluí–se que a partição π_α, não é uma qualquer partição de Z_1, ela tem as propriedades indicadas no Lema 2.20.

Atribui–se de seguida uma designação a estas propriedades.

Definição 2.21. Seja $\mathcal{M} = (Z, I, O, \delta, \beta, z_0)$ um autómato e seja π uma partição de Z. Diz–se que π é *admissível* ou que, possuí a *propriedade de substituição* se para todo o $X \in \pi$ e $i \in I$, existe $Y \in \pi$ tal que:

$$\delta(X,i) \subseteq Y. \tag{2.12}$$

Definição 2.22. Seja $\mathcal{M} = (Z, I, O, \delta, \beta, z_0)$ um autómato e seja π uma partição de Z. Diz–se que π é um *output consistente* se para todo o $X \in \pi$, $i \in I$ e $x, y \in X$:

$$\beta(x,i) = \beta(y,i). \tag{2.13}$$

De seguida, apresenta–se um exemplo de uma partição com estas duas propriedades.

Exemplo 2.23. Considere–se a partição $\pi_1 = \Big\{\{q_0,q_1\},\{q_2\},\{q_3\}\Big\}$ definida no Exemplo 2.18.

Verifica–se que, para o bloco $\{q_0,q_1\}$, $\delta_1(\{q_0,q_1\},a) = \{q_0,q_1\} \subseteq \{q_0,q_1\} \in \pi_1$ e $\delta_1(\{q_0,q_1\},b) = \{q_2\} \subseteq \{q_2\} \in \pi_1$. Não é necessário verificar os outros blocos de π_1, porque são conjuntos singulares. Logo, a partição π_1 tem a propriedade de substituição.

Verifica–se agora que π_1 é *output* consistente.

Para o bloco $\{q_0, q_1\}$, $\beta_1(q_0, a) = 1 = \beta_1(q_1, a)$ e $\beta_1(q_0, b) = 0 = \beta_1(q_1, b)$. Não é necessário verificar os outros blocos de π_1, uma vez que são conjuntos singulares. Assim, concluí–se que π_1 é *output* consistente.

Portanto, a partição π_1 é uma partição de Z_1 que tem a propriedade de substituição e é *output* consistente. ♢

Verifica–se que a propriedade de substituição e a propriedade de *output* consistente, são equivalentes à S–relação de equivalência $\Theta(\pi)$ ser uma congruência.

Comece–se então por verificar que a propriedade de compatibilidade da operação δ é equivalente à propriedade de substituição.

Lema 2.24. *Seja $\mathcal{M} = (Z, I, O, \delta, \beta, z_0)$ uma Σ_{aut}–álgebra e seja π uma partição de Z. As seguintes afirmações são equivalentes:*

1. *Para qualquer $x, y \in Z$ e para qualquer $i, i' \in I$, se $x\ R_\pi\ y$ e $i\ R_I\ i'$ então*

$$\delta(x, i)\ R_\pi\ \delta(y, i'); \tag{2.14}$$

2. *π tem a propriedade de substituição.*

Demonstração. Seja $X \in \pi$ e $i \in I$. Como $X \neq \emptyset$ então, existe $x \in X$. Considere–se $y = \delta(x, i)$ e seja $Y \in \pi$ o bloco da partição tal que $y \in Y$.

Seja $y' \in \delta(X, i)$. Então, existe $x' \in X$ tal que $y' = \delta(x', i)$. Deste modo, $x, x' \in X$. E portanto, $x\ R_\pi\ x'$ e $i\ R_I\ i$. Então por, (2.14) $\delta(x, i)\ R_\pi\ \delta(x', i)$. Como $y = \delta(x, i)$ e $y' = \delta(x', i)$ então $y\ R_\pi\ y'$ e portanto, $y' \in Y$.

Prova–se agora a implicação recíproca. Sejam $x, y \in Z$ e $i, i' \in I$. Suponha–se que $x\ R_\pi\ y$ e $i\ R_I\ i'$ (isto é, $i = i'$, pois R_I é a relação diagonal). Seja $X \in \pi$ tal que $x \in X$. Sabe–se que existe $Y \in \pi$ tal que $\delta(X, i) \subseteq Y$. Como $x\ R_\pi\ y$ então $y \in X$, e portanto $\delta(y, i) \in Y$. Assim, $\delta(x, i)\ R_\pi\ \delta(y, i')$. □

Verifica–se agora que a propriedade de compatibilidade da operação β é equivalente à propriedade de *output* consistente.

Lema 2.25. *Seja $\mathcal{M} = (Z, I, O, \delta, \beta, z_0)$ uma Σ_{aut}–álgebra e seja π uma partição de Z. As seguintes afirmações são equivalentes:*

1. *Para qualquer $x, y \in Z$ e para qualquer $i, i' \in I$, se $x\ R_\pi\ y$ e $i\ R_I\ i'$ então*

$$\beta(x, i)\ R_O\ \beta(y, i'), \tag{2.15}$$

2. π é output consistente.

Demonstração. Sejam $X \in \pi$, $i \in I$ e $x, y \in X$. Donde $x\ R_\pi\ y$ e $i\ R_I\ i$. Então, por (2.15) $\beta(x,i)\ R_O\ \beta(y,i)$. Como R_O é relação diagonal então $\beta(x,i) = \beta(y,i)$.

Prova–se agora a implicação recíproca. Sejam $x, y \in Z$ e $i, i' \in I$. Suponha–se que $x\ R_\pi\ y$ e $i\ R_I\ i'$. Seja $X \in \pi$, o bloco da partição π tal que, $x \in X$. Como $x\ R_\pi\ y$ então $x, y \in X$ e como $i\ R_I\ i'$ então $i = i'$. Portanto, $\beta(x,i) = \beta(y,i)$. E deste modo, $\beta(x,i)\ R_O\ \beta(y,i')$, pois R_O e R_I são relações diagonais. □

Introduz–se agora a definição de *partição induzida por* Φ.

Definição 2.26. Sejam $\mathcal{M}_1 = (Z_1, I_1, O_1, \delta_1, \beta_1, z_1)$ e $\mathcal{M}_2 = (Z_2, I_2, O_2, \delta_2, \beta_2, z_2)$ Σ_{aut}–álgebras e $\Phi = (\alpha, \tau, \theta)$ um homomorfismo de redução entre $\mathcal{M}_1$ e $\mathcal{M}_2$. A *partição induzida por* Φ é a partição de Z_1 definida por:

$$\pi_\Phi = \{\alpha^{-1}(z) \mid z \in Z_2\}.$$

Observe–se que a relação de equivalência induzida por π_Φ em $\mathcal{M}_1$ é precisamente o núcleo de Φ.

A Proposição que se apresenta de seguida é o caso particular do Teorema 1.18 do Capítulo 1, para os autómatos e homomorfismos de redução.

Proposição 2.27. *Sejam $\mathcal{M}_1 = (Z_1, I_1, O_1, \delta_1, \beta_1, z_1)$ e $\mathcal{M}_2 = (Z_2, I_2, O_2, \delta_2, \beta_2, z_2)$ Σ_{aut}–álgebras e $\Phi = (\alpha, \tau, \theta)$ um homomorfismo de redução entre $\mathcal{M}_1$ e $\mathcal{M}_2$. π_Φ tem a propriedade de substituição e é output consistente.*

Demonstração. A demonstração desta Proposição é consequência imediata do Teorema 1.18 do Capítulo 1.

□

Lema 2.28. *Sejam $\mathcal{M}_1 = (Z_1, I_1, O_1, \delta_1, \beta_1, z_1)$ e $\mathcal{M}_2 = (Z_2, I_2, O_2, \delta_2, \beta_2, z_2)$ Σ_{aut}–álgebras e $\Phi = (\alpha, \tau, \theta)$ um homomorfismo de redução entre $\mathcal{M}_1$ e $\mathcal{M}_2$. E seja $\mathcal{M}' = (\pi_\alpha, I_1, O_1, \delta', \beta', z_1)$ a Σ_{aut}–álgebra isomorfa a $\mathcal{M}_2$. Então, para todo $X, X' \in \pi_\Phi$, $i \in I_1$ e $o \in O_1$, tem-se:*

1. $\delta'(X,i) = X' \Leftrightarrow \delta_1(X,i) \subseteq X'$

2. $\beta'(X,i) = \{o\} \Leftrightarrow \beta_1(X,i) = \{o\}$

Demonstração. No Lema 2.20 provou–se uma implicação, portanto agora provar–se–á a implicação contrária. Começa–se por provar a condição 1. do Lema.

Suponha–se que $X \in \pi_\Phi$ e $i \in I$. Seja $\delta_1(X,i) \subseteq X'$ e suponha–se $\delta'(X,i) = X''$. Pela condição 1. do Lema 2.20, vem que $\delta_1(X,i) \subseteq X''$, e assim $\delta_1(X,i) \subseteq X' \cap X''$. Como $\delta_1(X,i) \neq \emptyset$ então $X' \cap X'' \neq \emptyset$. Como X' e X'' são blocos da mesma partição, então $X' = X''$. Portanto,

$$\delta_1(X,i) \subseteq X' \Rightarrow \delta'(X,i) = X'. \tag{2.16}$$

Prova–se agora a condição 2. do Lema.

Suponha–se que $\beta_1(X,i) = \{o\}$ e $\beta'(X,i) = \{o'\}$. Então pela condição 2., do Lema 2.20, $\beta_1(X,i) = \{o'\}$ e portanto, $\{o'\} = \{o\}$. Logo,

$$\beta_1(X,i) = \{o\} \Rightarrow \beta'(X,i) = \{o\}. \tag{2.17}$$

E fica assim provado o Lema. □

Define–se agora a Σ_{aut}–álgebra *quociente*. Seja $\mathcal{M} = (Z, I, O, \delta, \beta, z_0)$ uma Σ_{aut}–álgebra e considere–se a partição π em Z, com a propriedade de substituição e *output* consistente. Então, pode–se considerar a Σ_{aut}–álgebra *quociente* de $\mathcal{M}$ por π, como a Σ_{aut}–álgebra:

$$\mathcal{M}/\pi := \mathcal{M}/\Theta(\pi) = (\pi, I, O, \delta_\pi, \beta_\pi, z_0).$$

Para autómatos, em termos da partição π, as funções δ_π e β_π são definidas da seguinte forma:

1. $\delta_\pi(X,i) = Y$ se e só se $\delta(X,i) \subseteq Y$
2. $\beta_\pi(X,i) = \{o\}$ se e só se $\beta(X,i) = \{o\}$

Exemplo 2.29. Considere–se o autómato $\mathcal{M}_1$, que se apresenta no Exemplo 2.17. E considere–se uma partição de Z_1 definida por $\pi_2 = \Big\{\{q_0,q_1\},\{q_2,q_3\}\Big\}$. Esta partição tem a propriedade de substituição, uma vez que:

$$\delta_1(\{q_0,q_1\},a) = \{q_0,q_1\} \subseteq \{q_0,q_1\} \in \pi_2;$$

$$\delta_1(\{q_0,q_1\},b) = \{q_2\} \subseteq \{q_2,q_3\} \in \pi_2;$$

$$\delta_1(\{q_2,q_3\},a) = \{q_0,q_1\} \subseteq \{q_0,q_1\} \in \pi_2;$$

$$\delta_1(\{q_2,q_3\},b) = \{q_3\} \subseteq \{q_2,q_3\} \in \pi_2.$$

Para além disso, esta partição é *output* consistente, pois:

$$\beta_1(q_0,a) = 1 = \beta_1(q_1,a);$$

$$\beta_1(q_0,b) = 0 = \beta_1(q_1,b);$$

$$\beta_1(q_2, a) = 0 = \beta_1(q_3, a);$$

$$\beta_1(q_2, b) = 1 = \beta_1(q_3, b).$$

Portanto, pode–se construir o autómato quociente $\mathcal{M}_1/\pi_2$, sendo a partição π_2 o seu conjunto de estados. O diagrama de transições do autómato quociente apresenta–se na Figura 2.16.

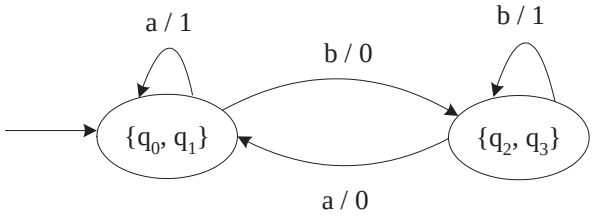


Figura 2.16: Diagrama de transições do autómato $\mathcal{M}_1/\pi_2$.

♢

Seja $\mathcal{M} = (Z, I, O, \delta, \beta, z_0)$ uma Σ_{aut}–álgebra e π uma partição de Z tal que $\Theta(\pi) = (R_\pi, R_I, R_O)$ é uma congruência em $\mathcal{M}$. A aplicação canónica ou natural $\nu_{\Theta(\pi)} : \mathcal{M} \longrightarrow \mathcal{M}/\Theta(\pi)$ é um Σ–homomorfismo sobrejectivo, onde $\nu_{\Theta(\pi)} = (\alpha_{R_\pi}, \tau_{R_I}, \theta_{R_O})$ com $\alpha_{R_\pi}(z) = z/R_\pi$ e τ_{R_I} e θ_{R_O} são funções identidade.

Em termos de partições, se se considerar π uma partição de Z com a propriedade de substituição e *output* consistente, a aplicação natural é definida por:

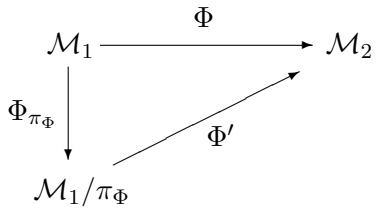
$$\Phi_\pi : \mathcal{M} \longrightarrow \mathcal{M}/\pi \tag{2.18}$$

onde $\Phi_\pi = (\alpha_\pi, \tau_\pi, \theta_\pi)$ é um homomorfismo de redução sobrejectivo e tal que, $\alpha_\pi(z) = X \Leftrightarrow z \in X$, com $X \in \pi$ e τ_π e θ_π são funções identidade.

O homomorfismo de redução Φ_π designa–se por *redução natural* de $\mathcal{M}$ para $\mathcal{M}/\pi$.

Se $\Phi = (\alpha, \tau, \theta)$ é um homomorfismo de redução entre $\mathcal{M}_1$ e $\mathcal{M}_2$ e π_Φ é a partição induzida por Φ em Z_1, que tem a propriedade de substituição e é *output* consistente, então pode–se construir a Σ_{aut}–álgebra $\mathcal{M}'$ como sendo a Σ_{aut}–álgebra quociente de $\mathcal{M}_1$ por π_Φ, isto é $\mathcal{M}' = \mathcal{M}_1/\pi_\Phi$.

Assim, sendo $\mathcal{M}_1 = (Z_1, I_1, O_1, \delta_1, \beta_1, z_1)$ e $\mathcal{M}_2 = (Z_2, I_2, O_2, \delta_2, \beta_2, z_2)$ Σ_{aut}–álgebras e $\Phi = (\alpha, \tau, \theta)$ um homomorfismo de redução entre $\mathcal{M}_1$ e $\mathcal{M}_2$, vai existir um isomorfismo $\Phi' = (\alpha', \tau', \theta')$ que está definido entre $\mathcal{M}_1/\pi_\Phi$ e $\mathcal{M}_2$ e que é tal que, $\Phi = \Phi' \circ \Phi_{\pi_\Phi}$, isto é:



Por conseguinte, verifica–se que o Primeiro Teorema do Homomorfismo se aplica aos autómatos de *Mealy*.

4 Equivalência comportamental

Sendo $\mathcal{M}_1$ e $\mathcal{M}_2$ dois autómatos de *Mealy*, quando se diz que estes autómatos fazem o mesmo, o que se pretende dizer na realidade? E que conclusões se pode retirar sobre autómatos, se eles fizerem o mesmo? Regressa–se assim às relações entre autómatos, mas neste momento analisar–se–á os seus comportamentos e não as suas estruturas. Dois autómatos efectuam o mesmo se tiverem o mesmo comportamento. Isto é, se o autómato $\mathcal{M}_2$ tiver o mesmo comportamento que o autómato $\mathcal{M}_1$, então para todo o $x \in Z_1$ e $w \in I_1^*$ tem de existir um $y \in Z_2$ tal que, $\beta_2^*(y, w) = \beta_1^*(x, w)$. E por sua vez, se o autómato $\mathcal{M}_1$ tiver o mesmo comportamento que o autómato $\mathcal{M}_2$ então para todo o $y \in Z_2$ e $w \in I_1^*$ tem de existir um $x \in Z_1$ tal que, $\beta_1^*(x, w) = \beta_2^*(y, w)$. Ou seja, o *output* gerado pelos dois autómatos quando recebem uma mesma palavra de *input* tem que ser igual. Assim, inicia–se esta secção estabelecendo em que circunstâncias duas Σ_{aut}–álgebras são *comportamentalmente equivalentes*.

Definição 2.30. Sejam $\mathcal{M}_1 = (Z_1, I_1, O_1, \delta_1, \beta_1, z_1)$ e $\mathcal{M}_2 = (Z_2, I_2, O_2, \delta_2, \beta_2, z_2)$ Σ_{aut}–álgebras. Diz–se que $\mathcal{M}_1$ e $\mathcal{M}_2$ são *comportamentalmente equivalentes* se $I_1 = I_2$, $O_1 = O_2$ e existe uma relação $R \subseteq Z_1 \times Z_2$ entre $\mathcal{M}_1$ e $\mathcal{M}_2$ que satisfaz as seguintes condições:

1. Domínio$(R) = \{x \in Z_1 \ : \ x \ R \ y \text{ para algum } y \in Z_2\} = Z_1$;
2. Contradomínio$(R) = \{y \in Z_2 \ : \ x \ R \ y \text{ para algum } x \in Z_1\} = Z_2$;
3. para $x \in Z_1$ e $y \in Z_2$, se $x \ R \ y$ então, para todo o $w \in I_1^*$, $\beta_1^*(x, w) = \beta_2^*(y, w)$;
4. $z_1 \ R \ z_2$.

A relação R designa–se por *equivalência comportamental* entre $\mathcal{M}_1$ e $\mathcal{M}_2$.

Para indicar que as Σ_{aut}–álgebras $\mathcal{M}_1$ e $\mathcal{M}_2$ são comportamentalmente equivalentes escreve–se: $\mathcal{M}_1 \equiv \mathcal{M}_2$.

Facilmente se prova que a relação $\equiv$ é uma relação de equivalência. Para provar que $\equiv$ é reflexiva, basta considerar a relação R como sendo a relação diagonal. Para provar que $\equiv$ é simétrica, considera–se a relação inversa de R. Por fim, para provar que $\equiv$ é transitiva, considera–se R como sendo a relação composta de duas relações S e T.

Proposição 2.31. *Sejam $\mathcal{M}_1 = (Z_1, I_1, \delta_1, z_1, F_1)$ e $\mathcal{M}_2 = (Z_2, I_2, \delta_2, z_2, F_2)$ autómatos finitos determinísticos. E seja $\mathcal{M}'_1 = (Z_1, I_1, O_1, \delta_1, \beta_1, z_1)$ o autómato de Mealy equivalente a $\mathcal{M}_1$ e $\mathcal{M}'_2 = (Z_2, I_2, O_2, \delta_2, \beta_2, z_2)$ o autómato de Mealy equivalente a $\mathcal{M}_2$. Se $\mathcal{M}'_1 \equiv \mathcal{M}'_2$ então $L(\mathcal{M}_1) = L(\mathcal{M}_2)$.*

Demonstração. Seja $L(\mathcal{M}_1)$ a linguagem reconhecida por $\mathcal{M}_1$. Como o autómato $\mathcal{M}'_1$ é equivalente ao autómato $\mathcal{M}_1$ então os autómatos $\mathcal{M}_1$ e $\mathcal{M}'_1$ reconhecem a mesma linguagem, ou seja $L(\mathcal{M}_1) = L(\mathcal{M}'_1)$. Como por hipótese, $\mathcal{M}'_1 \equiv \mathcal{M}'_2$ então para cada palavra $w \in I_1^*$, $\beta_1^*(z_1, w) = \beta_2^*(z_2, w)$ e portanto, $L(\mathcal{M}'_1) = L(\mathcal{M}'_2)$. Por sua vez, o autómato $\mathcal{M}'_2$ é equivalente ao autómato $\mathcal{M}_2$, então os autómatos $\mathcal{M}'_2$ e $\mathcal{M}_2$ reconhecem a mesma linguagem, isto é $L(\mathcal{M}'_2) = L(\mathcal{M}_2)$. Portanto, $L(\mathcal{M}_1) = L(\mathcal{M}'_1) = L(\mathcal{M}'_2) = L(\mathcal{M}_2)$. Assim, $L(\mathcal{M}_1) = L(\mathcal{M}_2)$. □

Veja–se agora alguns resultados acerca de Σ_{aut}–álgebras comportamentalmente equivalentes.

Proposição 2.32. *Sejam $\mathcal{M}_1 = (Z_1, I_1, O_1, \delta_1, \beta_1, z_1)$ e $\mathcal{M}_2 = (Z_2, I_2, O_2, \delta_2, \beta_2, z_2)$ Σ_{aut}–álgebras. Suponha-se que existe $\Phi = (\alpha, \tau, \theta)$ um homomorfismo de redução de $\mathcal{M}_1$ para $\mathcal{M}_2$ então $\mathcal{M}_1 \equiv \mathcal{M}_2$.*

Demonstração. Seja $\Phi = (\alpha, \tau, \theta)$ um homomorfismo de redução entre $\mathcal{M}_1$ e $\mathcal{M}_2$. Então $I_1 = I_2$ e $O_1 = O_2$. Portanto, resta provar que existe a relação $R \subseteq Z_1 \times Z_2$ entre $\mathcal{M}_1$ e $\mathcal{M}_2$. Para tal, sejam $x \in Z_1$, $y \in Z_2$ e $R \subseteq Z_1 \times Z_2$ a relação definida por:

$$x \; R \; y \Leftrightarrow \alpha(x) = y.$$

Daqui concluí–se que as condições 1. e 2. da Definição 2.30 se verificam, a condição 1. por α ser função e a condição 2. por α ser sobrejectiva. Verifica–se agora a condição 3.. Sejam $x \in Z_1$, $y \in Z_2$ tais que $x \; R \; y$ e seja $w \in I_1^*$ qualquer. Então:

$$\begin{aligned} \beta_1^*(x, w) &= \beta_2^*(\alpha(x), w), \text{ pois } \Phi \text{ é um homomorfismo de redução e pelo Lema 2.14} \\ &= \beta_2^*(y, w), \text{ pela definição de } R. \end{aligned}$$

Falta verificar a condição 4.. Como Φ é um homomorfismo então $\alpha(z_1) = z_2$. Portanto, pela forma como R foi definida, $z_1 \; R \; z_2$.

Assim, conclui–se que $\mathcal{M}_1 \equiv \mathcal{M}_2$. □

O recíproco desta Proposição não é verdadeiro. Caso fosse, seria a situação em que $\mathcal{M}_1 \equiv \mathcal{M}_2$ implicaria que $\mathcal{M}_1 \cong \mathcal{M}_2$. E isto nem sempre é verdade, basta ver o Exemplo 2.17, onde se definem dois autómatos $\mathcal{M}_1$ e $\mathcal{M}_2$ e um homomorfismo de redução Φ entre $\mathcal{M}_1$ e $\mathcal{M}_2$. Pela Proposição anterior, poderia–se logo concluir que $\mathcal{M}_1 \equiv \mathcal{M}_2$, mas não se poderia concluir que os autómatos são isomorfos. Se o fossem teria que existir uma bijecção entre Z_1 e Z_2, mas essa bijecção não pode existir uma vez que neste exemplo o número de elementos de Z_1 é diferente do número de elementos de Z_2.

Define–se agora Σ_{aut}–*álgebra reduzida*, com o intuito de apresentar mais alguns resultados acerca da equivalência comportamental de Σ_{aut}–álgebras.

Definição 2.33. Seja $\mathcal{M} = (Z, I, O, \delta, \beta, z_0)$ uma Σ_{aut}–álgebra. Diz–se que $\mathcal{M}$ é *reduzida* se para todo $x, y \in Z$, se $x \neq y$ então para algum $w \in I^*$, $\beta^*(x, w) \neq \beta^*(y, w)$.

A definição anterior, no caso dos autómatos é a definição de *autómato reduzido*.

Lema 2.34. *Sejam $\mathcal{M}_1 = (Z_1, I_1, O_1, \delta_1, \beta_1, z_1)$ e $\mathcal{M}_2 = (Z_2, I_2, O_2, \delta_2, \beta_2, z_2)$ Σ_{aut}–álgebras. Suponha–se que $\mathcal{M}_1 \equiv \mathcal{M}_2$ e que $\mathcal{M}_2$ é reduzida, então existe um homomorfismo de redução $\Phi = (\alpha, \tau, \theta)$ de $\mathcal{M}_1$ para $\mathcal{M}_2$.*

Demonstração. Suponha–se que $\mathcal{M}_1 \equiv \mathcal{M}_2$, sendo $R \subseteq Z_1 \times Z_2$ a equivalência comportamental entre $\mathcal{M}_1$ e $\mathcal{M}_2$. E suponha–se que $\mathcal{M}_2$ é uma Σ_{aut}–álgebra reduzida.

Se $\mathcal{M}_2$ é uma Σ_{aut}–álgebra reduzida, então a equivalência comportamental R será uma função de Z_1 para Z_2. Para verificar este facto, comece–se por notar que Domínio$(R) = Z_1$, pela condição 1. da Definição 2.30. Note–se também, que para todo o $z \in Z_1$ e $x, y \in Z_2$ se $z\ R\ x$ e $z\ R\ y$ então $x = y$. De facto, se $z\ R\ x$ então pela condição 3. da Definição 2.30, para todo o $w \in I_1^*$ $\beta_2^*(x, w) = \beta_1^*(z, w)$. Do mesmo modo, se $z\ R\ y$ então pela condição 3. da Definição 2.30, para todo o $w \in I_1^*$ $\beta_1^*(z, w) = \beta_2^*(y, w)$. Por conseguinte, se $z\ R\ x$ e $z\ R\ y$ então, para todo o $w \in I_1^*$ $\beta_2^*(x, w) = \beta_1^*(z, w) = \beta_2^*(y, w)$. Portanto, para todo o $w \in I_1^*$ $\beta_2^*(x, w) = \beta_2^*(y, w)$, o que pela Definição 2.33, para $x \neq y$ é impossível. Logo, $x = y$.

Defina–se $\alpha : Z_1 \longrightarrow Z_2$ por:

$$\alpha(z) = z' \Leftrightarrow z\ R\ z'$$

e sejam $\tau : I_1 \longrightarrow I_2$ e $\theta : O_1 \longrightarrow O_2$ funções identidade.

Repare–se ainda que Contradomínio$(R) = Z_2$ e portanto α é sobrejectiva. Para além disso, para todo o $w \in I_1^*$ α satisfaz a seguinte condição:

$$\beta_2^*(\alpha(z), w) = \beta_1^*(z, w), \tag{2.19}$$

pois por definição, $z\ R\ \alpha(z)$ e R é equivalência comportamental, como tal a condição 3. da Definição 2.30 verifica-se.

Tem–se que verificar também, que para $z_1 \in Z_1$ e $z_2 \in Z_2$, $\alpha(z_1) = z_2$. Como $\mathcal{M}_1 \equiv \mathcal{M}_2$, então pela condição 4. da definição 2.30, $z_1\ R\ z_2$. Donde $\alpha(z_1) = z_2$.

Mas, para que Φ seja efectivamente um homomorfismo de redução falta provar que:

$$\alpha(\delta_1(z,i)) = \delta_2(\alpha(z),i).$$

Seja $x = \alpha(\delta_1(z,i))$ e $y = \delta_2(\alpha(z),i)$. Pretende–se mostrar que $x = y$. Como $\mathcal{M}_2$ é reduzida, basta mostrar que para todo o $w \in I_1^*$, $\beta_2^*(x,w) = \beta_2^*(y,w)$. Esta condição verifica-se, se se conseguir mostrar que para qualquer $i \in I_2$,

$$\beta_2(\alpha(z),i) \cdot \beta_2^*(x,w) = \beta_2(\alpha(z),i) \cdot \beta_2^*(y,w) \tag{2.20}$$

e assim, pode–se eliminar $\beta_2(\alpha(z),i)$ em ambos os membros da equação. De facto, o que se efectuará é mostrar que ambos os membros da equação são iguais a $\beta_2^*(\alpha(z),iw)$. Isto é:

$$\begin{aligned}\beta_2^*(\alpha(z),iw) &= \beta_2(\alpha(z),i) \cdot \beta_2^*(\delta_2(\alpha(z),i),w), \text{ por definição de } \beta_2^* \\ &= \beta_2(\alpha(z),i) \cdot \beta_2^*(y,w), \text{ por definição de } y.\end{aligned}$$

e

$$\begin{aligned}\beta_2^*(\alpha(z),iw) &= \beta_1^*(z,iw), \text{ pela condição (2.19)} \\ &= \beta_1(z,i) \cdot \beta_1^*(\delta_1(z,i),w), \text{ por definição de } \beta_1^* \\ &= \beta_2(\alpha(z),i) \cdot \beta_2^*(\alpha(\delta_1(z,i)),w), \text{ pela condição (2.19)} \\ &= \beta_2(\alpha(z),i) \cdot \beta_2^*(x,w), \text{ por definição de } x.\end{aligned}$$

Assim, fica provado que Φ é um homomorfismo de redução. □

O Corolário seguinte permite verificar quando é que dois autómatos são isomorfos. Neste caso, o Corolário é apresentado para autómatos de *Mealy* e não para as Σ_{aut}–álgebras, de forma a garantir que os conjuntos de estados são finitos.

Corolário 2.35. *Sejam $\mathcal{M}_1 = (Z_1, I_1, O_1, \delta_1, \beta_1, z_1)$ e $\mathcal{M}_2 = (Z_2, I_2, O_2, \delta_2, \beta_2, z_2)$ autómatos de Mealy. Suponha–se que $\mathcal{M}_1 \equiv \mathcal{M}_2$ e que $\mathcal{M}_1$ e $\mathcal{M}_2$ são autómatos reduzidos então $\mathcal{M}_1 \cong \mathcal{M}_2$.*

Demonstração. Como $\mathcal{M}_1 \equiv \mathcal{M}_2$ e $\mathcal{M}_2$ é um autómato reduzido, então pelo Lema 2.34 existe um homomorfismo de redução $\Phi_1 = (\alpha_1, \tau_1, \theta_1)$ de $\mathcal{M}_1$ para $\mathcal{M}_2$. Como $\equiv$ é uma relação de equivalência, então $\mathcal{M}_2 \equiv \mathcal{M}_1$. Dado que $\mathcal{M}_1$ é um autómato reduzido, então pelo Lema 2.34 existe um homomorfismo de redução $\Phi_2 = (\alpha_2, \tau_2, \theta_2)$ de $\mathcal{M}_2$ para $\mathcal{M}_1$. Como $\alpha_1 : Z_1 \longrightarrow Z_2$ é sobrejectiva e $\alpha_2 : Z_2 \longrightarrow Z_1$ também é, Z_1 e Z_2 têm o mesmo número de elementos, assim α_1 e α_2 são bijecções e portanto Φ_1 e Φ_2 são isomorfismos.

Assim tem–se que $\mathcal{M}_1 \cong \mathcal{M}_2$, por exemplo pelo isomorfismo Φ_1. (Note–se que τ_1 e θ_1 são funções identidade, pelo facto de Φ_1 ser homomorfismo de redução.) □

Regresse–se agora à situação em que $\mathcal{M}_2$ não é um autómato reduzido. O que se pretende fazer é juntar os conjuntos de estado cujos elementos têm o mesmo comportamento, dando origem a um novo autómato que será reduzido. Começa–se então por definir uma relação de equivalência que associa num conjunto de estados, elementos com o mesmo comportamento.

Definição 2.36. Seja $\mathcal{M} = (Z, I, O, \delta, \beta, z_0)$ uma Σ_{aut}–álgebra e seja $x, y \in Z$. Então, $x \equiv_\ell^{\mathcal{M}} y$ se para todo o $w \in I^*$,

$$\beta^*(x, w) = \beta^*(y, w). \tag{2.21}$$

Lema 2.37. *A relação $\equiv_\ell^{\mathcal{M}}$ é uma relação de equivalência.*

Demonstração. Para verificar que $\equiv_\ell^{\mathcal{M}}$ é uma relação de equivalência, tem que se verificar que $\equiv_\ell^{\mathcal{M}}$ é reflexiva, simétrica e transitiva.

Começa–se por verificar que $\equiv_\ell^{\mathcal{M}}$ é reflexiva. Para qualquer $x \in Z$ e $w \in I^*$, $\beta^*(x, w) = \beta^*(x, w)$ e portanto, $x \equiv_\ell^{\mathcal{M}} x$. Logo, $\equiv_\ell^{\mathcal{M}}$ é reflexiva.

Verifica–se agora a simetria. Sejam $x, y \in Z$ e suponha–se que $x \equiv_\ell^{\mathcal{M}} y$. Então, para todo o $w \in I^*$, $\beta^*(x, w) = \beta^*(y, w)$. Logo, $\beta^*(y, w) = \beta^*(x, w)$ para todo o $w \in I^*$. Deste modo, $y \equiv_\ell^{\mathcal{M}} x$. Logo, $\equiv_\ell^{\mathcal{M}}$ é simétrica.

Verifica–se agora a transitividade. Sejam x, y e $z \in Z$ e suponha–se que $x \equiv_\ell^{\mathcal{M}} y$ e $y \equiv_\ell^{\mathcal{M}} z$. Então, para todo o $w \in I^*$, $\beta^*(x, w) = \beta^*(y, w)$ e $\beta^*(y, w) = \beta^*(z, w)$. Portanto, para todo o $w \in I^*$, $\beta^*(x, w) = \beta^*(z, w)$. Portanto, $x \equiv_\ell^{\mathcal{M}} z$. Logo, $\equiv_\ell^{\mathcal{M}}$ é transitiva. Assim, conclui–se que $\equiv_\ell^{\mathcal{M}}$ é uma relação de equivalência. □

Proposição 2.38. *Seja $\mathcal{M} = (Z, I, O, \delta, \beta, z_0)$ uma Σ_{aut}–álgebra. A relação $\equiv_\ell^{\mathcal{M}}$ é uma equivalência comportamental entre $\mathcal{M}$ e $\mathcal{M}$.*

Demonstração. Uma vez que a relação $\equiv_\ell^{\mathcal{M}}$ é uma relação de equivalência verifica–se que, Domínio($\equiv_\ell^{\mathcal{M}}$) = Contradomínio($\equiv_\ell^{\mathcal{M}}$) = Z e que $z_0 \ \equiv_\ell^{\mathcal{M}} \ z_0$.

Para além disso, pela forma como $\equiv_\ell^{\mathcal{M}}$ foi definida, verifica–se que, para $x, y \in Z$ se $x \ \equiv_\ell^{\mathcal{M}} \ y$ então, para todo o $w \in I^*$, $\beta^*(x, w) = \beta^*(y, w)$.

Fica assim provado que $\equiv_\ell^{\mathcal{M}}$ é uma equivalência comportamental entre $\mathcal{M}$ e $\mathcal{M}$. □

Sendo $\mathcal{M} = (Z, I, O, \delta, \beta, z_0)$ uma Σ_{aut}–álgebra e dado que $\equiv_\ell^{\mathcal{M}}$ é uma relação de equivalência, então esta induz uma partição em Z, que se designa por $\rho_{\mathcal{M}}$ e é tal que $\rho_{\mathcal{M}} = Z/\equiv_\ell^{\mathcal{M}}$.

Lema 2.39. *Seja $\mathcal{M} = (Z, I, O, \delta, \beta, z_0)$ uma Σ_{aut}–álgebra e seja $\rho_{\mathcal{M}}$ a partição induzida por $\equiv_\ell^{\mathcal{M}}$ em Z. Então, $\rho_{\mathcal{M}}$ tem a propriedade de substituição e é output consistente.*

Demonstração. Seja $X \in \rho_{\mathcal{M}}$ e $z \in X$. Se $i \in I$, então existe um bloco $Y \in \rho_{\mathcal{M}}$, tal que $\delta(z, i) \in Y$. Começa–se por mostrar que, $\delta(X, i) \subseteq Y$. Para tal, mostrar–se–á que, se $z \equiv_\ell^{\mathcal{M}} z'$ então $\delta(z, i) \equiv_\ell^{\mathcal{M}} \delta(z', i)$. Considere–se $z' \in X$, tal que $z \equiv_\ell^{\mathcal{M}} z'$. Pela definição de $\equiv_\ell^{\mathcal{M}}$, se w é um qualquer elemento de I^* então,

$$\beta^*(z, iw) = \beta^*(z', iw). \tag{2.22}$$

Mas, por definição de β^*,

$$\beta^*(z, iw) = \beta(z, i) \cdot \beta^*(\delta(z, i), w). \tag{2.23}$$

Do mesmo modo,

$$\beta^*(z', iw) = \beta(z', i) \cdot \beta^*(\delta(z', i), w). \tag{2.24}$$

Substituindo as condições (2.23) e (2.24), na condição (2.22), obtém–se:

$$\beta(z, i) \cdot \beta^*(\delta(z, i), w) = \beta(z', i) \cdot \beta^*(\delta(z', i), w). \tag{2.25}$$

Mas, pela condição (2.21), como $z \equiv_\ell^{\mathcal{M}} z'$, vem que: $\beta^*(z, i) = \beta^*(z', i)$. Então em particular,

$$\beta(z, i) = \beta(z', i)$$

Assim, eliminando $\beta(z, i)$ em ambos os membros da equação (2.25), obtém–se para todo o $w \in I^*$:

$$\beta^*(\delta(z, i), w) = \beta^*(\delta(z', i), w),$$

e deste modo, $\delta(z, i) \equiv_\ell^{\mathcal{M}} \delta(z', i)$ como se queria provar. Portanto, $\rho_{\mathcal{M}}$ tem a propriedade de substituição.

Falta provar que $\rho_{\mathcal{M}}$ é *output* consistente. Para tal, suponha–se que $X \in \rho_{\mathcal{M}}$ e considere–se $z, z' \in X$. Então, $z \equiv_\ell^{\mathcal{M}} z'$. Portanto, para qualquer $i \in I$ obtém–se: $\beta^*(z, i) = \beta^*(z', i)$, e em particular

$$\beta(z, i) = \beta(z', i).$$

Deste modo, $\rho_{\mathcal{M}}$ é *output* consistente. □

Pela condição (2.18) e pelo Lema anterior, se $\mathcal{M} = (Z, I, O, \delta, \beta, z_0)$ é uma Σ_{aut}–álgebra e a partição $\rho_{\mathcal{M}}$ induzida por $\equiv_\ell^{\mathcal{M}}$ em Z, tem a propriedade de substituição e é *output*

consistente então, vai existir um homomorfismo de redução $\Phi_{\rho_\mathcal{M}} = (\alpha_{\rho_\mathcal{M}}, \tau_{\rho_\mathcal{M}}, \theta_{\rho_\mathcal{M}})$ que está definido de $\mathcal{M}$ para $\mathcal{M}/\rho_\mathcal{M}$, e que é dado por:

$$\Phi_{\rho_\mathcal{M}} : \mathcal{M} \longrightarrow \mathcal{M}/\rho_\mathcal{M} \tag{2.26}$$

onde $\alpha_{\rho_\mathcal{M}}(z) = X \Leftrightarrow z \in X$ e $\tau_{\rho_\mathcal{M}}$ e $\theta_{\rho_\mathcal{M}}$ são funções identidade.

Ao construir a Σ_{aut}–álgebra $\mathcal{M}/\rho_\mathcal{M}$, tem–se como objectivo encontrar uma Σ_{aut}–álgebra reduzida e que está relacionada com $\mathcal{M}$. E de facto verifica–se que:

Proposição 2.40. *Seja $\mathcal{M} = (Z, I, O, \delta, \beta, z_0)$ uma Σ_{aut}–álgebra e seja $\rho_\mathcal{M}$ a partição induzida por $\equiv_\ell^\mathcal{M}$ em Z. Então, $\mathcal{M}/\rho_\mathcal{M}$ é uma Σ_{aut}–álgebra reduzida.*

Demonstração. Sejam $X_1, X_2 \in \rho_\mathcal{M}$, onde $\rho_\mathcal{M}$ é a partição induzida por $\equiv_\ell^\mathcal{M}$ em Z e suponha–se que, para todo o $w \in I^*$,

$$\beta^*_{\rho_\mathcal{M}}(X_1, w) = \beta^*_{\rho_\mathcal{M}}(X_2, w). \tag{2.27}$$

Pretende–se mostrar que, $X_1 = X_2$. Como X_1 e X_2 são classes de equivalência da partição induzida por $\equiv_\ell^\mathcal{M}$, então é suficiente mostrar que $x \equiv_\ell^\mathcal{M} y$, para alguns $x \in X_1$ e $y \in X_2$. De facto $x, y \in X_1 \cap X_2$, pois caso X_1 e X_2 fossem distintos então $X_1 \neq X_2$ e isto não é o que se pretende. Portanto, seja $\Phi_{\rho_\mathcal{M}} = (\alpha_{\rho_\mathcal{M}}, \tau_{\rho_\mathcal{M}}, \theta_{\rho_\mathcal{M}})$ a redução natural definida de $\mathcal{M}$ para $\mathcal{M}/\rho_\mathcal{M}$. Sejam ainda $x \in X_1$ e $y \in X_2$. Então, $\alpha_{\rho_\mathcal{M}}(x) = X_1$ e $\alpha_{\rho_\mathcal{M}}(y) = X_2$. Como $\Phi_{\rho_\mathcal{M}}$ é um homomorfismo de redução, então para todo o $w \in I^*$,

$$\begin{aligned} \beta^*_{\rho_\mathcal{M}}(X_1, w) &= \beta^*_{\rho_\mathcal{M}}(\alpha_{\rho_\mathcal{M}}(x), w), \text{ pois } \alpha_{\rho_\mathcal{M}}(x) = X_1 \\ &= \beta^*(x, w), \text{ pois } x \in X_1. \end{aligned}$$

e

$$\begin{aligned} \beta^*_{\rho_\mathcal{M}}(X_2, w) &= \beta^*_{\rho_\mathcal{M}}(\alpha_{\rho_\mathcal{M}}(y), w), \text{ pois } \alpha_{\rho_\mathcal{M}}(y) = X_2 \\ &= \beta^*(y, w), \text{ pois } y \in X_2. \end{aligned}$$

Assim, por aplicação da condição (2.27) deduz–se que $\beta^*(x, w) = \beta^*(y, w)$, para todo o $w \in I^*$. E portanto, $x \equiv_\ell^\mathcal{M} y$. □

As Proposições e Teorema seguintes são apresentadas só para os autómatos de *Mealy*.

Proposição 2.41. *Sejam $\mathcal{M}_1 = (Z_1, I_1, O_1, \delta_1, \beta_1, z_1)$ e $\mathcal{M}_2 = (Z_2, I_2, O_2, \delta_2, \beta_2, z_2)$ autómatos de Mealy e sejam $\rho_{\mathcal{M}_1}$ a partição induzida por $\equiv_\ell^{\mathcal{M}_1}$ em Z_1 e $\rho_{\mathcal{M}_2}$ a partição induzida por $\equiv_\ell^{\mathcal{M}_2}$ em Z_2. $\mathcal{M}_1 \equiv \mathcal{M}_2$ implica que $\mathcal{M}_1/\rho_{\mathcal{M}_1} \cong \mathcal{M}_2/\rho_{\mathcal{M}_2}$.*

Demonstração. Pela condição (2.26), verifica–se que existem os homomorfismos de redução, $\Phi_1 : \mathcal{M}_1 \longrightarrow \mathcal{M}_1/\rho_{\mathcal{M}_1}$ e $\Phi_2 : \mathcal{M}_2 \longrightarrow \mathcal{M}_2/\rho_{\mathcal{M}_2}$. Por conseguinte, pela Proposição 2.32, $\mathcal{M}_1/\rho_{\mathcal{M}_1} \equiv \mathcal{M}_1$ e $\mathcal{M}_2 \equiv \mathcal{M}_2/\rho_{\mathcal{M}_2}$. Consequentemente, como $\equiv$ é uma relação de

equivalência e $\mathcal{M}_1 \equiv \mathcal{M}_2$, vem que: $\mathcal{M}_1/\rho_{\mathcal{M}_1} \equiv \mathcal{M}_2/\rho_{\mathcal{M}_2}$. Mas, pela Proposição 2.40, $\mathcal{M}_1/\rho_{\mathcal{M}_1}$ e $\mathcal{M}_2/\rho_{\mathcal{M}_2}$ são autómatos reduzidos. Por isso, pelo Corolário 2.35, $\mathcal{M}_1/\rho_{\mathcal{M}_1} \cong \mathcal{M}_2/\rho_{\mathcal{M}_2}$. Fica provada a Proposição. □

Teorema 2.42. *Sejam $\mathcal{M}_1 = (Z_1, I_1, O_1, \delta_1, \beta_1, z_1)$ e $\mathcal{M}_2 = (Z_2, I_2, O_2, \delta_2, \beta_2, z_2)$ autómatos de Mealy. $\mathcal{M}_1 \equiv \mathcal{M}_2$ se e só se existe o autómato $\mathcal{M}_3 = (Z_3, I_3, O_3, \delta_3, \beta_3, z_3)$ e homomorfismos de redução $\Phi : \mathcal{M}_1 \longrightarrow \mathcal{M}_3$ e $\Psi : \mathcal{M}_2 \longrightarrow \mathcal{M}_3$.*

Demonstração. Suponha–se que existe um homomorfismo de redução $\Phi : \mathcal{M}_1 \longrightarrow \mathcal{M}_3$ e que existe um homomorfismo de redução $\Psi : \mathcal{M}_2 \longrightarrow \mathcal{M}_3$. Então, pela Proposição 2.32 $\mathcal{M}_1 \equiv \mathcal{M}_3$ e $\mathcal{M}_2 \equiv \mathcal{M}_3$. Como $\equiv$ é uma relação de equivalência, então $\mathcal{M}_1 \equiv \mathcal{M}_2$.

Suponha–se que $\mathcal{M}_1 \equiv \mathcal{M}_2$ e seja $\mathcal{M}_3 = \mathcal{M}_2/\rho_{\mathcal{M}_2}$. Então, pela condição (2.26) existe um homomorfismo de redução $\Psi : \mathcal{M}_2 \longrightarrow \mathcal{M}_3$.

Falta agora mostrar que existe um homomorfismo de redução $\Phi : \mathcal{M}_1 \longrightarrow \mathcal{M}_3$. Para isso, considere–se o autómato quociente $\mathcal{M}_1/\rho_{\mathcal{M}_1}$. Então, pela condição (2.26) existe um homomorfismo de redução $\Lambda : \mathcal{M}_1 \longrightarrow \mathcal{M}_1/\rho_{\mathcal{M}_1}$. Como por hipótese $\mathcal{M}_1 \equiv \mathcal{M}_2$ então, pela Proposição 2.41 $\mathcal{M}_1/\rho_{\mathcal{M}_1} \cong \mathcal{M}_3$ e portanto, existe um isomorfismo Γ que está definido de $\mathcal{M}_1/\rho_{\mathcal{M}_1}$ para $\mathcal{M}_3$. Deste modo, definindo $\Phi = \Gamma \circ \Lambda$ vem que, $\Phi : \mathcal{M}_1 \longrightarrow \mathcal{M}_3$ é o isomorfismo composto, e em particular é um homomorfismo de redução. Logo, existem os homomorfismos de redução Φ e Ψ. □

Assim, pode–se dizer que $\mathcal{M}/\rho_{\mathcal{M}}$ é de certo modo o mais pequeno e possível autómato, que "efectua o mesmo"que o autómato $\mathcal{M}$.

Proposição 2.43. *Sejam $\mathcal{M}_1 = (Z_1, I_1, O_1, \delta_1, \beta_1, z_1)$ e $\mathcal{M}_2 = (Z_2, I_2, O_2, \delta_2, \beta_2, z_2)$ autómatos de Mealy. Considere–se $\rho_{\mathcal{M}_1}$ a partição induzida por $\equiv_\ell^{\mathcal{M}_1}$ em Z_1. Se existe um homomorfismo de redução $\Phi : \mathcal{M}_1 \longrightarrow \mathcal{M}_2$ então, existe um homomorfismo de redução $\Phi' : \mathcal{M}_2 \longrightarrow \mathcal{M}_1/\rho_{\mathcal{M}_1}$.*

Demonstração. Como existe um homomorfismo de redução $\Phi : \mathcal{M}_1 \longrightarrow \mathcal{M}_2$, então pela Proposição 2.32 $\mathcal{M}_1 \equiv \mathcal{M}_2$. Por sua vez, pela condição (2.26) verifica–se que existe um homomorfismo de redução, $\Phi''' : \mathcal{M}_2 \longrightarrow \mathcal{M}_2/\rho_{\mathcal{M}_2}$. Dado que $\equiv$ é uma relação de equivalência então $\mathcal{M}_2 \equiv \mathcal{M}_1$. E portanto, pela Proposição 2.41 existe um isomorfismo Φ'' definido de $\mathcal{M}_2/\rho_{\mathcal{M}_2}$ para $\mathcal{M}_1/\rho_{\mathcal{M}_1}$. Sendo assim, definindo $\Phi' = \Phi'' \circ \Phi'''$, tem–se um homomorfismo de redução de $\mathcal{M}_2$ para $\mathcal{M}_1/\rho_{\mathcal{M}_1}$, como se pretendia mostrar. □

Esta proposição mostra que se pode encontrar um único autómato mais pequeno, que vai ter o mesmo comportamento que um autómato de $\mathcal{M}$.

Teorema 2.44. *Sejam $\mathcal{M}_1 = (Z_1, I_1, O_1, \delta_1, \beta_1, z_1)$ e $\mathcal{M}_2 = (Z_2, I_2, O_2, \delta_2, \beta_2, z_2)$ autómatos de Mealy tais que, $I_1 = I_2$ e $O_1 = O_2$. E sejam $\rho_{\mathcal{M}_1}$ a partição induzida por $\equiv_\ell^{\mathcal{M}_1}$ em Z_1 e $\rho_{\mathcal{M}_2}$ a partição induzida por $\equiv_\ell^{\mathcal{M}_2}$ em Z_2. $\mathcal{M}_1 \equiv \mathcal{M}_2$ se e só se, existe um isomorfismo $i : \mathcal{M}_1/\rho_{\mathcal{M}_1} \longrightarrow \mathcal{M}_2/\rho_{\mathcal{M}_2}$, onde $i = (i_Z, i_I, i_O)$, sendo i_I e i_O funções identidade.*

Demonstração. Suponha–se que $\mathcal{M}_1 \equiv \mathcal{M}_2$. Pela Proposição 2.41, existe o isomorfismo $i : \mathcal{M}_1/\rho_{\mathcal{M}_1} \longrightarrow \mathcal{M}_2/\rho_{\mathcal{M}_2}$ tal que, i_I e i_O são funções identidade.

Suponha–se que existe um isomorfismo $i : \mathcal{M}_1/\rho_{\mathcal{M}_1} \longrightarrow \mathcal{M}_2/\rho_{\mathcal{M}_2}$, com i_I e i_O funções identidade. Assim, em particular i é um homomorfismo de redução de $\mathcal{M}_1/\rho_{\mathcal{M}_1}$ para $\mathcal{M}_2/\rho_{\mathcal{M}_2}$. E portanto, pela Proposição 2.32 $\mathcal{M}_1/\rho_{\mathcal{M}_1} \equiv \mathcal{M}_2/\rho_{\mathcal{M}_2}$. Pela condição (2.26), verifica–se ainda que existem homomorfismos de redução $\Phi_1 : \mathcal{M}_1 \longrightarrow \mathcal{M}_1/\rho_{\mathcal{M}_1}$ e $\Phi_2 : \mathcal{M}_2 \longrightarrow \mathcal{M}_2/\rho_{\mathcal{M}_2}$. Assim, pela Proposição 2.32, $\mathcal{M}_1 \equiv \mathcal{M}_1/\rho_{\mathcal{M}_1}$ e $\mathcal{M}_2 \equiv \mathcal{M}_2/\rho_{\mathcal{M}_2}$. Como $\equiv$ é uma relação de equivalência, se $\mathcal{M}_1 \equiv \mathcal{M}_1/\rho_{\mathcal{M}_1}$ e $\mathcal{M}_1/\rho_{\mathcal{M}_1} \equiv \mathcal{M}_2/\rho_{\mathcal{M}_2}$ então $\mathcal{M}_1 \equiv \mathcal{M}_2/\rho_{\mathcal{M}_2}$. Ainda por $\equiv$ ser uma relação de equivalência, se $\mathcal{M}_1 \equiv \mathcal{M}_2/\rho_{\mathcal{M}_2}$ e $\mathcal{M}_2/\rho_{\mathcal{M}_2} \equiv \mathcal{M}_2$ então $\mathcal{M}_1 \equiv \mathcal{M}_2$, como se queria provar. □

Conclusões e trabalho futuro

Neste trabalho definiu–se um autómato finito como uma álgebra heterogénea e verificou–se que conceitos, como homomorfismo, isomorfismo, congruência e álgebra quociente também se aplicam para autómatos. Reformulou–se o Primeiro Teorema do Homomorfismo para autómatos, usando para isso as ferramentas habituais do estudo de autómatos.

Como continuação deste trabalho seria importante estender esta teoria aos autómatos de pilha e/ou às máquinas de *Turing*, definindo estas máquinas como álgebras.

Um autómato de pilha é um séptuplo $\mathcal{M} = (Z, I, \Gamma, \delta, z_0, q_0, F)$ onde Z é o conjunto de estados, I é o alfabeto de *input*, Γ é o alfabeto da pilha, δ é uma aplicação definida de $Z \times (I \cup \{\varepsilon\}) \times \Gamma^*$ no conjunto dos subconjuntos finitos de $Z \times \Gamma^*$, z_0 é o estado inicial do autómato, q_0 é uma constante de Γ designada por símbolo inicial da pilha e $F \subseteq Z$ é o conjunto de estados finais.

Mais do que tudo isto, seria interessante reformular resultados, ferramentas e conceitos que são tradicionalmente estudados na teoria de autómatos de pilha, no contexto da álgebra universal, de forma análoga ao que foi efectuado nesta tese para os autómatos de *Mealy*.

Bibliografia

[1] S. Burris and H.P. Sankappanavar, *A course in universal algebra*, Graduate Texts in Mathematics, Vol. 78, New York - Heidelberg Berlin, Springer - Verlag, (1981).

[2] K. Denecke and S.L. Wismath, *Universal algebra and applications in theoretical computer science*, Boca Raton, Florida, Chapman & Hall/CRC, (2002).

[3] L. Descalço, A. Madeira, M. A. Martins, *Algebraic logic view of automata*, Department of Mathematics, University of Aveiro, (2009).

[4] G. Grätzer, *Universal algebra*, 2nd ed., New York, Heidelberg, Berlin: Springer-Verlog, (1979).

[5] V. B. Kudryavtsev and I. G. Rosenberg, *Structural theory of automata, semigroups and universal algebra*, Series II: Mathematics, Physics and Chemistry, Vol. 207, Springer, (2003).

[6] W. M. L. Holcombe, *Algebraic automata theory*, Cambridge University Press, (1982).

[7] J.E. Hopcroft and J.D. Ullman, *Introduction to automata theory, languages and computation*, Addison-Wesley, (1979).

[8] J.M. Howie, *Automata and languages*, Oxford University Press, (1991).

[9] K. Meinke and J.V. Tucker, *Universal algebra*, In Hanbook of logic in computer science, Vol. 1, pages 189-411, Oxford University Press, New York, (1992).

[10] D. Sannella and A. Tarlecki, *Foundations of algebraic specifications and formal program development*, Cambridge University Press, (a aparecer).

[11] M.W. Shields, *An introduction to automata theory*, Blackwell Scientific Publications, (1987).